JINNAH INSTITUTE

POLICY BRIEF

January 18, 2017

OPEN DEMOCRACY INITIATIVE

In this Issue

Analysing the differences in defining offences , penalties, and procedural mechanisms prescribed under PECB

By Daanika Kamal

Policing Cybercrime: A Comparative Analysis of the Prevention of Electronic Crimes Bill

Introduction

Despite uncertainty and questions over implementation and investigation mechanisms, the Pakistan's Prevention of Electronic Crimes Bill (2016)[1] became operational just days after it was passed. The first case of cybercrime surfaced in Khyber Pakhtunkhwa, where a man was arrested for blackmailing women by uploading fake videos on social media websites[2]. Under the PECB, the accused was taken in for cyber-stalking and spoofing. More recently, a University professor was arrested for harassing a female teacher under Section 21 of the PECB[3], which includes offences against the modesty of a person.

In comparison to similar cybercrime bills around the world, PECB mandates harsher penalties for offences, and goes one step further to criminalize acts which are not considered unlawful in comparable nation-states. Clauses aim to restrict internet freedoms, curbing freedom of speech, access to information and the right to privacy. The need to balance legislation on cybercrime while ensuring freedom of speech remain key concerns, and are likely to impact the already restricted space for public discourse.

For the scope of this brief, PECB has been compared to similar legislation in the United States[4], United Arab Emirates[5] and India[6]. The US law applies to majority of social media companies which have branched out to Pakistan in recent years and is therefore important to use as a comparative point for examination. India mirrors Pakistan's governmental structure, which allows for a political lens into the drafting of the PECB. And UAE's socio-religious stance, as incorporated into aspects of its national legislation, brings a different dimension to the legal analysis.

International Law and Transnational Cooperation

International law encourages States to be party to human rights instruments which include provisions limiting freedom of expression in cases where it is used to incite violence, terrorism, genocide or war propaganda. In cyber offences, the transnational

nature of digital data makes it difficult to establish uniformity in criminalization under international jurisdiction. Digital content which is legal to distribute in one country, may be illegal in another. National jurisdiction, therefore, is the major regulatory authority in defining, investigating and penalizing electronic crimes. However, it is important that the leeway granted to nation-states are not only appropriate, but also proportionate to protections awarded by multilateral instruments.

Over 80 countries have signed or ratified a binding cybercrime instrument that has directly or indirectly influenced national laws. The International Covenant on Civil and Political Rights[7] and the Council of Europe Convention on Cybercrime[8] are the two main frameworks referred to by States when developing electronic crime policies. Membership in multilateral cybercrime initiatives therefore encourages nation-states to develop relevant legislation for purposes of international cooperation, amongst others.

'International cooperation' falls under Section 42 of the PECB, which grants the Federal Government authority to extend cooperation to any foreign government or international organization that request information for purposes of investigation or proceedings of offences relating to information systems. Under this provision, digital data of Pakistani citizens collected through audio, visual, text or other digital formats can be forwarded to the pertaining party without seeking prior permission from the Court. Section 42 may be seen as a testament to Pakistan's efforts towards 'international cooperation,' as specified in the Preamble of the PECB. However, despite claiming synergy, many of the PECB's sections are inconsistent with the ICCPR.

International Standards: Criminalization of Offences

Most offences included in cybercrime legislation fall under three main umbrella themes: *access, interception and interference, or content-related offences.* While there is a general consensus regarding the broader areas of criminalization internationally, provisions in domestic legislation are approached differently. Under *access,* illegally accessing information systems or digital data differ according to the object of offence, requirement of intent and resulting loss or damage. Requirement of intent also varies in the approaches taken by States to criminalize *interception and interference.* Under these offences, respective authorities are concerned with whether or not the offence is restricted to non-public data, whether data was tampered with, and whether 'recklessness' is cause for penalty. Content-related crimes particularly employ human rights provisions, including the freedom of expression and the right to information. In principle, digital content is subject to the same regulations as traditional print media and speech, as "freedom of expressions is applicable regardless of frontiers and through any media of one's choice."[9] In practice however, nation-states are at the liberty to decide if *content-related offences* are criminalized under cyber legislation.

Many offences and resulting penalties are influenced by varying boundaries to freedom of expression, stemming from country-specific religious norms, public morals and ensuing values. Socio-cultural elements of limitations placed on rights and freedoms are generally reflected in national laws, accounting for the differences in provisions. Although most countries adopt legislation for fraud, forgery and identity offences, content-related acts such as hate speech, transmission of sexually explicit material, spamming and cyber-stalking are less commonly found. Differences also arise in

definitions used within the law, production versus distribution of related data, and possession versus access of contentious content.

Of provisions relevant to cybercrime, offences considered punishable under International Human Rights Law include acts that incite national, racial or religious hatred[10], any war propaganda[11], and the production or distribution of child pornography[12]. Exceptions to international human rights law are usually subject to the 'margin of appreciation[13],' if interferences are prescribed in domestic laws and are necessary for a well-functioning democratic society. The margin is established using a cultural frame of reference, by examining the right involved and the purpose such interference is anticipated to shadow.

Due to lacking consensus in defining cybercrime, finding comparative statistics for various jurisdictions is difficult. However, comparing the language used, definitions presented, and penalties assigned to digital offences in national legislation allows for an interesting insight into the cultural and socio-political influences that either strengthen or impair legislative instruments in different countries.

For the scope of this brief, provisions in Pakistan's *Prevention of Electronic Crimes Bill (2016)* will be compared to similar clauses in India's *Information Technology Act (2008),* United Arab Emirates' *Federal Decree Law on Combating Cybercrimes (2006)* and the United States' *Code, Title 18.*

Definitions

Definitions of cybercrime tend to depend on the purpose of using the term. At the core, acts against the integrity and confidentiality of computer data are themselves not sufficient to prescribe a legal definition of the aggregate term. Cybercrime is better defined as a collection of acts, organized into categories depending on the material object of offence. In some cases, definitions prescribed to acts within cybercrime legislation may be considered interchangeable; however, transposable definitions pose a threat to the integrity and authoritative (mis)use of powers assigned to investigatory agencies. '*Access*,' '*dishonest intention*,' and '*critical infrastructure*' are three examples of varying definitions in electronic crime legislation which can present measurement challenges based on the vague and subjective nature of their text.

- *Dishonest intention:* The US, UAE and India cybercrime legislations do not include definitions for 'intent'. In UAE's case, the requirement of intent was entirely removed from Sections dealing with 'illegal access' to electronic information and replaced with 'prohibition'. Although the word 'intent' has been regularly used in Indian legislation, it has not been given its own definition in the text of the law. In Pakistan, the term 'dishonest intention' defined under Section 2 is a subjective expression at best. By including provisions such as '*intention to create hatred,'* the law is not only vague but subject to varying interpretations.

- *Critical infrastructure:* PECB is the only law of those examined which explicitly includes and defines critical infrastructure. Sections 6, 7 and 8 include the term, defining it as '*any other private or government infrastructure designated by the Government as*

critical infrastructure as may be prescribed under this Act'. Unauthorized access, transmission or interference with 'critical infrastructure' leaves heavy room for supposition, which when coupled with the broad definition enables the government to declare anything as 'critical,' as it deems suitable.

- *Access to data:* India's Information Technology Act (2008) defines 'access' as gaining entry into, instructing or communicating with the function resources of a computer system or network. Under PECB definitions, access to data includes 'gaining control' of data, but goes one step further to incorporate the 'ability to read or use' data generated by information systems. UAE and US laws repeatedly use the word access to describe cyber offences, but derive it's meaning from other national legislation.

Contemporary Cybercrime Provisions: Comparative Notes

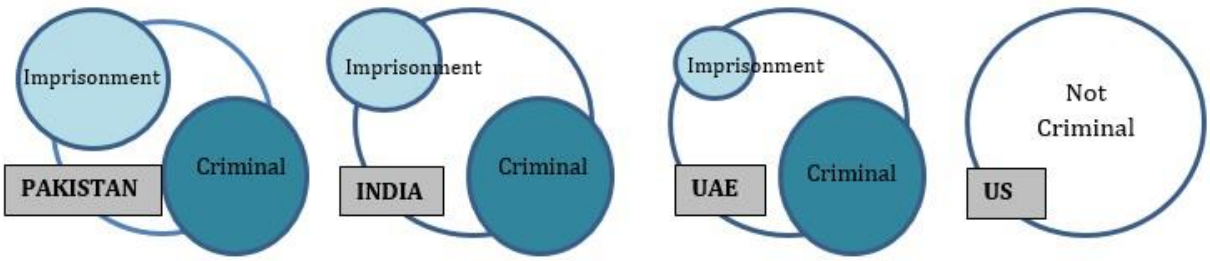
1) Cyber Terrorism

Many justify the existence of cybercrime bills primarily to curtail terrorism. However, the UAE and the US do not include any clause specifying cyber terrorism in their respective legislature. The UAE only mentions terrorism under Article 26, where the crime is defined by using digital networks to publish methods for manufacturing incendiary devices. On the other hand, India and Pakistan both include lengthy definitions of cyber terrorism.

India's ITA (2008) restricts its definition to accessibility concerns of critical information infrastructure. Section 66F includes illegal access, as well as obtaining and sharing restricted data. The PECB's definition of cyber terrorism however, includes coercion, intimidation and the creation of panic in society as an offence, in addition to the advancement of terrorist objectives. The main criticism here is that the law applies to those who commit, as well as those who *threaten* to commit the offences. With penalties ranging up to 14 years in prison and a 50 million rupees fine, vague definitions leave a lot of room for misinterpretation and misuse of the law which can incorrectly implicate citizens.

Corresponding to the wider definition of 'cyber terrorism', the PECB also includes a Section specific to the use of technology to recruit, fund or plan terrorism, and one specific to the glorification, praise or celebratory depiction relating to terrorism or terrorist organizations.

2) Hate Speech



While International law does not require criminalization of hate speech, it does guide States to prohibit national, racial or religious hatred which incites discrimination, hostility or violence[14]. In cases where such acts are criminalized, offences are sheltered under 'general offences' and not necessary specific to digital spaces. The decision to include religion, disability, sexual orientation or gender in hate crimes is solely at the discretion of the particular State.

International law, however, also provides a high threshold which must be met in order for the freedom of expression to be limited under 'hate speech'. In assessing the severity of speech, it is recommended that the context and content of the statement, requirement of intent (not including recklessness), and the degree of risk of resulting harm are adequately evaluated.

Even though the United States Code has no clause specifying (digital) hate speech, UAE's cyber laws regulate it via Article 24 of the Decree, defined as information which promotes hatred, racism, sectarianism, or damages national unity. The offence is punishable by temporary imprisonment and a fine not less than 500,000 dirhams. In India, hate speech falls under Section 66A of the ITA, which broadly categorizes it as the promoting of 'offensive messages through communication services'. If convicted, the accused could face up to 3 years in prison. However, unlike parallel laws in Pakistan, the offence is bailable in India. Under PECB's Article 11, anyone who prepares or disseminates information that advances inter-faith, sectarian or ethnic hatred can be imprisoned for up to 7 years.

3) Sexually Explicit Material

While all the countries in question have laws regulating the use of electronic mediums for the production and distribution of sexually explicit material, PECB has mandated a much higher punishment for such offences, extending from 5 to 10 years in prison. Indian legislation warrants 3 years in prison for those convicted of publishing 'obscene material' in electronic form, deeming the offence cognizable and bailable. For material which contains 'sexually explicit' material, the punishment rises up to 7 years in prison, and the accused is no longer eligible for bail. UAE's Decree Law groups pornography offences with gambling activities, but does not specify a time-frame for imprisonment of those convicted. In Article 18, however, the law includes the acquiring of pornographic materials, including those relating to juveniles, punishable by at least 6 months. The 'importation' and 'transportation' of obscene matters for distribution falls under Section 1462 of the US Code, indictable by up to 5 years.

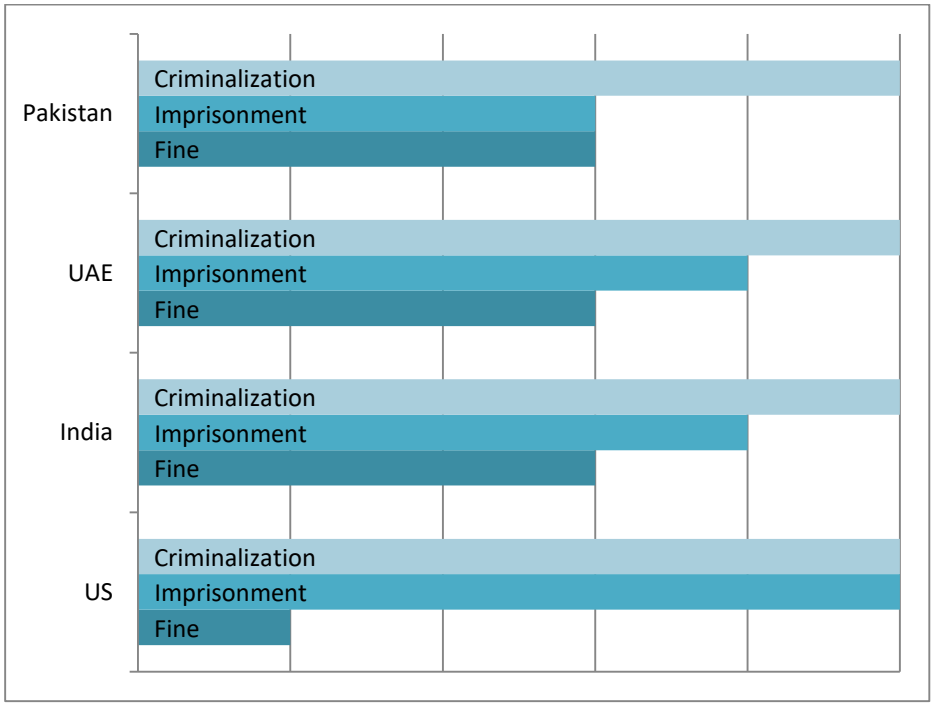
4) Child Pornography

Majority of images which contain child pornography are transmitted electronically as digital data through both bilateral and multilateral servers.[15] Almost all domestic legislation includes clauses criminalizing child pornography, though definitions of age, and acts covered in the law may differ marginally. It is important to note that most relevant articles in national cybercrime legislation refer to the term 'child' or 'minor' without specifying an age within the text itself. Applicable ages can be found in other domestic legislation, such as child protection laws or criminal laws.

Accordingly, all cybercrime laws examined follow clauses relating to sexually explicit material with clauses specifying child pornography. PECB's Article 21(2) includes *offences against modesty of natural person* which specify acts that include minors, increasing imprisonment to 10 years under a non-compoundable, non-bailable offence. Article 22 further defines child pornography, which includes the 'intentional' production, distribution

or 'offering' of materials which depict minors engaged in sexually explicit conduct. Indian legislation also recognizes children-related sexual material as a non-bailable offence, with a comparatively similar stance on penalties as those prescribed under PECB.

On the other hand, the US Code discusses child pornography in two separate instances; Section 1466A refers to the obscene representation of the sexual abuse of children, with imprisonment extending up to 20 years, and Section 2252A, which includes 'certain activities' constituting of child pornography, punishable under the same regulations. UAE does not use the Decree, but taps into other domestic legislature to regulate child pornography nationwide.



5) Violation of Privacy

US cyber law does not specify the invasion of privacy. While the PECB has not instituted a separate clause for the violation of privacy, Article 20 includes the criminalization of 'information that harms the reputation or privacy' of an individual. Similar to Indian legislation, the crime is punishable by up to three years in prison, as well as a fine. UAE's Decree Law has a reduced sentence of 6 months for similar crimes, but includes eavesdropping, recording, and photography for 'defamation' in its definition.

It is important to note here, however, that despite a lack of privacy-centered clause, the PECB also includes sections pertaining to the retention, preservation and acquisition of data, which has the potential to be misused and grossly violate the right to privacy of citizens. Under Section 31, 'authorized' officers can order the release of data from those operating information systems and preserve it for up to three months, prior to submission in Courts. This time frame allows sufficient opportunity for breach of information. Further, service providers are now required to retain data of customers for up to a year, and subject to a warrant, are to make it available to authorized agencies and officers. Previously, data could be retained for up to 90 days, and the PECB has increased this limit without specifying how the data will be secured from external breaches. With no legislation pertaining to privacy or data protection, the retention of traffic data could be significantly invasive to citizen rights and freedoms.

6) Spamming and Cyber-stalking

Internationally, digital spam is seen as an issue of consent rather than content. As a result, none of the binding multilateral instruments dealing with cybercrime criminalize provisions on spam. The EU Directive on Data Protection requires member States to take the measures necessary to ensure digital marketing and communication operates with the consent of consumers[16]. However, like other international mechanisms, the Directive does not require the establishment of a 'spamming' offence under domestic law.

Pakistan is the only country in those chosen for this comparative study which criminalizes 'spamming'. Under Article 25 of the PECB, spamming is defined as the transmission of harmful, misleading or unsolicited information to any person without permission of the recipient. If convicted, the accused could serve up to 3 months in prison. In 2014, the Indian Supreme Court removed Section 66A from the ITA, which criminalized the publishing of 'annoying' or 'offensive' content. Comparatively, this clause was very similar to spamming clauses under PECB, however, India found the section vague and constitutionally incompatible with freedom of expression.

PECB is also the only cybercrime law amongst the legislations chosen which criminalizes cyber stalking. The loose definition used for cyber stalking, that is, the 'intent to coerce, intimidate or harass a person using information systems' penalizes the offence with a fine of up to 1 million rupees, or imprisonment up to one year.

7) Forgery and Fraud (Offences Related to Identity)

Computer-related fraud and forgery criminalizes acts which infringe on financial assets, property and validity of documents.[17] Despite general legislation covering fraud and forgery, cybercrime acts have included specific clauses to extend conventional offences to a digital environment, focusing on the manipulation of data and a malicious intent requirement.

Of the countries in question, UAE legislation has the most subtle approach to forgery and fraud. Definitions used include 'fraudulent use of electronic networks,' with forgery only considered criminal if relating to electronic documents of federal or local governments. Impersonation is also included in Decree Law under Article 11. In comparison to the minor

penalties assigned to these cybercrimes by UAE, India and Pakistan both specify imprisonment for fraud for up to 2 or 3 years, respectively. For electronic forgery specifically, the PECB warrants imprisonment up to 7 years, significantly higher than penalties prescribed by India and the UAE. The US Code however takes it a step further, penalizing all crimes related to fraud or forgery by up to 15 years in prison.

Identity-related offences may also be regulated under similar provisions. Digital transactions have increased the chances of identity theft by accessing personal data online and forging information accordingly. Although many identity-related offences have not warranted their own clause in cybercrime legislation and are instead regulated under illegal access, data interference, or fraud and forgery, all bills examined in this brief found independent sections for acts related to identity. PECB and ITA both have similar penalties assigned to unauthorized use of identity information, subject to Article 16 and Section 66C and 66D, respectively. UAE's *Decree* targets impersonation and false personification under Article 11, while the US *Code* criminalizes 'aggravated' identity theft. It is, however, unclear how the term 'aggravated' is defined under US law.

Major Contentions with PECB: Freedom of Speech, Law Enforcement and Powers Awarded to PTA

In general, nation-states protect freedom of expression under constitutional law. In theory, such protections should be extended to both digital and non-digital forms of expression; however, the major contention with cyber laws is the limitation it places on the freedom of speech. Although there is not a set understanding of what legitimizes such restrictions, protecting national security, public safety, and limiting acts of terror are commonly found in national legislatures.

Pakistan criminalizes the act of displaying or transmitting information that harms the reputation of a person which could be construed to penalize satire, political expression or any other form of journalism. Although defamation exists under the Ordinance of 2002, Section 20 duplicates similar clauses without specifying exceptions or procedural norms, as other laws require. Misapplication of the law could lead to one of two possibilities: an increasing number of citizens facing trials and prison sentences, or a rise in the number of citizens using censorship as a means to protect themselves from the law, instead of the law protecting their freedom of speech.

The presence of a legal framework is not sufficient for effective enforcement of cybercrime laws. In addition, sufficient training for officers that defines the boundaries between investigative powers and intruding the individual's right to privacy, and supplying investigative authorities with the tools and techniques required to obtain evidence are all prerequisites for an adequate implementation of the law.

In matters of surveillance, international law requires jurisprudence to give sufficient information to gauge the conditions and circumstances under which authorities are sanctioned to use investigative measures. Jurisprudence should also include guarantees against the abuse of such powers, which not only render authorities competent to carry out actions but enable oversight of implementation measures.

Under section 37 of the PECB, the PTA has been granted unrestricted powers to remove any information transmitted via technology which is deemed as being 'anti-state' or implicates the 'glory of Islam'. The language used in this section is almost identical to Article 19 of the Constitution, however the legislative exclusions and procedural mechanisms stated in Article 19A award powers of interpretation to the parliament. Under PECB, interpretation of what

digital information warrants removal or blockage, as well as investigation under due process, is left to the PTA, an executive authority mandated to regulate the telecommunication and internet industry.

Comparatively, interpretation of the law is internationally considered to be a function of the judiciary. Granting judicial and parliamentary powers to an executive body has not been seen in any other jurisdiction. Such an unmitigated transfer of powers enable's the PTA to not only place unreasonable restrictions on the use of digital mediums but has the potential to curb access to entire digital spaces for information in trying to block one specific piece of content. The blanket ban on YouTube that resulted from blocking access to specific 'unlawful' content, for example, is testament to PTA's inability to effectively deal with information on digital platforms.

Subsection 2 of Section 20, 21 and 22 not only grant discretionary powers to the PTA, but specify that any aggrieved person may apply to the Authority to make content-based decisions and determine appropriate remedies for complaints. Given that usual procedural actions require Courts to hear the merit of the case prior to determining penalties, the PTA will be unable to provide effective relief to the aggrieved, as it lacks jurisdiction over the various platforms it would need to implicate.

Conclusion

Due to technological advances, the risks of cyber threats have multiplied. National infrastructures are increasingly more vulnerable to compromises, prompting countries to establish legislation regulating the use of technology. But the balance between the need to legislate against criminal activity in the realm of technology and the internet, and the need to ensure personal freedoms enshrined in the Constitution are not infringed, is necessary. Reviewing legislations of various jurisdictions indicate inconsistencies in how cybercrime is defined, what risks and threats fall under the scope of cybercrime, and the development of information and communication technologies in the modern age. Estimating the potential damage of cyber threats to infrastructures, businesses and individuals may be miscalculated, and this miscalculation is reflected in the prescribed judicial sentences and enforcement mechanisms defined under law.

In comparison to India, UAE and the US, the PECB has the highest number of crimes included under law, specifies harsher penalties and awards unrestricted authority to investigate and prosecute. Establishing such high punishments violates the rule of proportionality. While the stated objective of the Bill is to counter crimes relating to information technologies, most provisions are left open to interpretation, leaving wide open the possibility of the laws being used to curb freedom of expression, and associated fundamental rights via the internet. This is even more worrisome as the internet and new media make up a large part of social and political discourse today. The inclusion of explicit definitions and greater clarity in offences in the Bill is increasingly necessary to avoid subjective terms and limit the space granted to authorities to interpret the law as they deem suitable.

References

[1] Prevention of Electronic Crimes Bill. (2016, April 13). Retrieved, June 2, 2016, from http://www.na.gov.pk/uploads/documents/1462252100_756.pdf
[2] K-P police book first cybercrime suspect over Facebook harassment - The Express Tribune. Available at: http://tribune.com.pk/story/1162788/k-p-police-book-first-cybercrime-suspect/
[3] KU professor arrested for online harassment of female teacher- Dawn News. Available at: http://www.dawn.com/news/1288627
[4] Cybercrime Laws of the United States. Compiled October 2006 by Al Rees, CCIPS. Available at http://www.oas.org/juridico/spanish/us_cyb_laws.pdf.
[5] UAE. Federal Decree Law No. 5 of 2012, On Combating Cybercrimes. Available at: http://www.ejustice.gov.ae.
[6] India Information Technology (Amendment) Act 2008. Available at: http://www.eprocurement.gov.in/news/Act2008.pdf
[7] UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171
[8] Council of Europe, *Convention on Cybercrime*, 23 November 2001, available at: http://www.refworld.org/docid/47fdfb202.html
[9] United Nations Human Rights Council, 2012. Resolution 20/8 on The promotion, protection and enjoyment of human rights on the Internet, A/HRC/RES/20/8, 16 July 2012.
[10] ICCPR Art 20(2)
[11] ICCPR Art 20(1)
[12] OP-CRC-SC Art (3)
[13] Legg, A., 2012. The Margin of Appreciation in International Human Rights Law. Oxford: Oxford Monographs in International Law.
[14] ICCPR Article 20
[15] UNODC, 2010. The Globalisation of Crime. A Transnational Organized Crime Threat Assessment. Chapter 10. Available at: http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf, p.212.
[16] EU Directive on Data Protection, Article 13(3)
[17] Sieber, U., 1998. Legal Aspects of Computer-Related Crime in the Information Society COMCRIME-Study. Available at: www.edc.uoc.gr/~panas/PATRA/sieber.pdf.