Cyber Crime and Data Retention

COE Convention nr 185 on cybercrime

- Concluded in Budapest on 23 November 2001
- First comprehensive instrument underlining the seriousness of cybercrime and the possible remedies
- Defines a series of offences i.e. illegal access, illegal interception, attacks on the integrity of data and data systems, abuse of computer systems, information fraude, child pornography, intellectual property infringements …
- It further calls for the introduction of criminal sanctions ,the collection of electronic evidence , data retention measures and mutual legal assistance in this area

Cyber Crime and Data Retention

COE Convention nr 189 protocol to the Convention on cybercrime concerning the criminalisation of acts of racist and xenophobic nature

- Supplementing the Cybercrime Convention regarding the criminalisation of acts of racist and xenophobic nature
- Qualifies racist and xenophobic material, its dissemination through computer systems, threats and insults, crimes against humanity

Cyber Crime and Data Retention

Council Decision 2000/375/JHA of 29 May 2000 to combat child pornography on the Internet

Aim

- to intensify measures to prevent and combat the production, processing, possession and distribution of child pornography material through the Internet
- Promote the effective investigation and prosecution of offences in this area
- Contains measures to encourage Internet users to inform law enforcement authorities on suspected distribution of child pornography material on the Internet
- Calls for the setting up at national level of specialised law enforcement units dealing with child pornography
- Obliges law enforcement authorities to act swiftly when information is received on suspected production, possession and distribution of child pornography

Chapter 24 Presentation

Cyber Crime and Data Retention

Means

- Ensure effective cooperation to facilitate effective investigation and prosecuriton
- Establish points of contact on a 24/7 basis consisting of knowledgeable personnel as well as specialised law enforcement units
- Inform Europol, within the limits of its mandate, of suspected cases
- Engage in a dialogue with industry to eleiminate child pornography from the Internet by f.i. advise or withdraw on child pornography material, retain traffic data, set up control systems
- Monitor technological developments in order to modify legislation or to initiate new legislation

Cyber Crime and Data Retention

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

Aim

- To improve cooperation between judicial and other competent authorities, including the police and other special law enforcement authorities, through the approximation of rules on criminal law in the area of attacks against information system

Chapter 24 Presentation

Cyber Crime and Data Retention

Means

- Imposes measures to ensure that illegal access to information systems, illegal system interference, illegal data interference, or the instigation aiding and attempts to conduct the aforementioned are punishable as a criminal offence, at least for cases which are not minor
- Those offences should be punishable by effective, proportional and dissuasive criminal penalties – for some criminal penalties of a maximum of at least between one and three years of imprisonment
- Provides for higher criminal penalities when these offences are committed within the frawework of a criminal organisation (defined in Joint Action 98/733/JHA) or when they have caused serious damages or affected essential interests
- Obligation to establish points of contact for the exchange of information on a 24/7 basis
- Implementation deadline is 16 March 2007

Cyber Crime and Data Retention

Directive of the EP and the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC

Aim

- To harmonise the provisions of MS concerning obligation on the providers of publicly available electronic communication services or of a public communication network with respect to he retention of certain data which are generated or processed by them in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by MS in national law
- Shall apply to traffic and location data as well as data necessary to identify the subscriber or registered user – it does not apply to the content of electronic communications

Chapter 24 Presentation

Cyber Crime and Data Retention

Means

- Creates an obligation on operators to retain traffic and location data
- Access to data is only provided to competent nationallauthorities in specific cases and in accordance with national law
- Contains the various categories of data to be retained
- Data needs to be retained for periods of not less than 6 months and for a maximum of two years from the date of the communication
- Appropriate measures need to be taken regarding data protection and data security
- Data needs to be stored in such a way that a swift transmission to the competent authorities is ensured

Cyber Crime and Data Retention

Means (continued)

- Statistics on the requests and transmission, including the time period will need to be provided
- Art 15 of the data protection Direcitve 2002/58/EC is amended to take into account this directive
- A certain flexibility is granted to those MS that want to retain data for longer periods than the max 2 years – a notification procedure is enacted
- An evaluation will take place within 3 years – implementation is scheduled 18 months after the adoption and an additional 18 months can be obtained for Internet communications