Cybercrime: the state of legislation

UN Commission for Crime Prevention and Criminal Justice, Side-event
Vienna International Centre, Tuesday, 15 May 2018, 9h00h – 9h50, Conference Room M3

Agenda

1. From 2013 to 2018: overview of progress made in the adoption of legislation on cybercrime and electronic evidence
2. Laws on cybercrime and electronic evidence: what is needed?
   - Substantive criminal law: offences against and by means of computers
   - Procedural powers for law enforcement to secure electronic evidence
   - Human rights and rule of safeguards
3. How to go about developing and adopting legislation?
4. Lessons learnt

www.coe.int/cybercrime

Speakers

Cristina Schulman, Vice-Chair of the Cybercrime Convention Committee, Ministry of Justice, Romania

Jayantha Fernando, Information and Communication Technology Agency, Sri Lanka

Marcos Salt, University of Buenos Aires, Ministry of Justice, Argentina

Pedro Verdelho, Office of the Prosecutor General, Portugal

Graham Willmott, Head of Cybercrime Unit, European Commission

Alexander Seger, Cybercrime Division, Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Substantive criminal law on cybercrime: developments 2013 - 2018

Background / Council of Europe:

- **Cybercrime Convention Committee + capacity building ► Cooperation with 160+ countries**
- **Reviews of legislation**
- **Octopus Community (www.coe.int/cybercrime) ► Country WIKIs**
- **Cursory overview of state of legislation January 2013 / January 2018***
- **Benchmarks:**
  - **Articles 2-12 Budapest Convention (for criminalisation)**
  - **Articles 16-21 Budapest Convention (for procedural powers**

* By Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania

Substantive criminal law on cybercrime: developments 2013 - 2018

Reforms of legislation on cybercrime and electronic evidence in most UN m/s in recent years

		Reforms underway or in recent years*			
	States	By January 2013		By January 2018	
All Africa	54	25	*46%*	45	*83%*
All Americas	35	25	*71%*	31	*89%*
All Asia	42	34	*81%*	37	*88%*
All Europe	48	47	*98%*	48	*100%*
All Oceania	14	12	*86%*	12	*86%*
All	**193**	**143**	***74%***	**173**	***90%***

Substantive criminal law on cybercrime: developments 2013 - 2018

By January 2013	States	Largely in place		Partially in place		Not in place or no information	
All Africa	54	6	11%	18	33%	30	56%
All Americas	35	10	29%	12	34%	13	37%
All Asia	42	13	31%	17	40%	12	29%
All Europe	48	38	79%	8	17%	2	4%
All Oceania	14	3	21%	6	43%	5	36%
All	**193**	**70**	**36%**	**61**	**32%**	**62**	**32%**

By January 2018	States	Largely in place		Partially in place		Not in place or no information	
All Africa	54	14	26%	21	39%	19	35%
All Americas	35	14	40%	15	43%	6	17%
All Asia	42	17	40%	18	43%	7	17%
All Europe	48	44	92%	4	8%	0	0%
All Oceania	14	5	36%	6	43%	3	21%
All	**193**	**94**	**49%**	**64**	**33%**	**35**	**18%**

Substantive criminal law on cybercrime: developments 2013 - 2018

- Good progress in terms of substantive criminal law against Articles 2 – 12 Budapest Convention
- By January 2018, almost half of UN m/s had substantive criminal law provisions in place
- More detailed analyses required
- Strengthening of criminal justice capacities needed to apply legislation

Substantive criminal law on cybercrime: developments 2013 - 2018

Concern: Laws on cybercrime used to prosecute speech, media

- The protection of national security and public order is a legitimate ground for restricting freedom of expression where that restriction is
  - prescribed by law
  - necessary in a democratic society
  - proportionate
- Broad, vaguely defined provisions do not meet these requirements
  - "use of computers with intent to compromise the independence of the state or its unity, integrity, safety or any of its high economic, political, social, military or security interests or subscribe, participate, negotiate, promote, contract or deal with an enemy in any way in order to destabilise security and public order or expose the country to danger …"
  - "use of computers to create chaos in order to weaken the trust of the electronic system of the state or provoke or promote armed disobedience, provoke religious or sectarian strife, disturb public order, or harm the reputation of the country … "
  - "creation of sites with a view to disseminating ideas contrary to public order or morality"
  - "broadcasting information to mislead security forces"
- Problematic trend ► Discredits legitimate action on cybercrime ► violates fundamental rights

Procedural law on e-evidence: developments 2013 - 2018

- **Limited progress regarding specific procedural powers – reliance on general powers – problem of safeguards**

Specific procedural powers		In January 2013		In January 2018	
	States	Largely in place		Largely in place	
All Africa	54	5	*9%*	10	*19%*
All Americas	35	5	*14%*	9	*26%*
All Asia	42	8	*19%*	13	*31%*
All Europe	48	31	*65%*	39	*81%*
All Oceania	14	1	*7%*	3	*21%*
All	**193**	**50**	***26%***	**74**	***38%***

Discussion

Agenda

- **Laws on cybercrime and electronic evidence: what is needed?**
  - **Substantive criminal law: offences against and by means of computers**
  - **Procedural powers for law enforcement to secure electronic evidence**
  - **Human rights and rule of safeguards**
- **How to go about developing and adopting legislation?**
- **Lessons learnt?**

Speakers

Cristina Schulman, Vice-Chair of the Cybercrime Convention Committee, Ministry of Justice, Romania

Jayantha Fernando, Information and Communication Technology Agency, Sri Lanka

Marcos Salt, University of Buenos Aires, Ministry of Justice, Argentina

Pedro Verdelho, Office of the Prosecutor General, Portugal

Graham Willmott, Head of Cybercrime Unit, European Commission

Alexander Seger, Cybercrime Division, Council of Europe

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE