UiO : Faculty of Law
University of Oslo

Development of EU Cybersecurity Law: A Tale of Lemons, Turf, Surf and Grey Boxes

Lee A. Bygrave
Professor of Law, Director of Norwegian Research Center for Computers and Law

Cybersecurity Conference, Maastricht University, Brussels, 22.06.2023

‘Wicked problems’ (Rittel & Webber)

- ‘[T]he problems of governmental planning—and especially those of social or policy planning—are ill-defined; and they rely upon elusive political judgment for resolution. (Not ‘solution’. Social problems are never solved. At best they are only re-solved—over and over again.)’.
- ‘As we seek to improve the effectiveness of actions in pursuit of valued outcomes, as system boundaries get stretched, and as we become more sophisticated about the complex workings of open societal systems, it becomes ever more difficult to make the planning idea operational’.

Security economics

‘Securitization’ as underlying narrative

- security given progressively greater priority at expense of other interests
- state actors employ increasingly stringent measures, in reaction to threat situation presented in increasingly alarmist tones

Turf war(s)

‘The Union…shall respect their [MS] essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State’.

– Art 4(2) TEU

Turf war(s) [2]

Debates over which actors to be covered by EU cybersec law

- E.g. NISD coverage: EP proposed ‘food supply chain’ as constituent of essential services; Council opposed this

Regulatory swell

EU cybersec law: from low to high swell

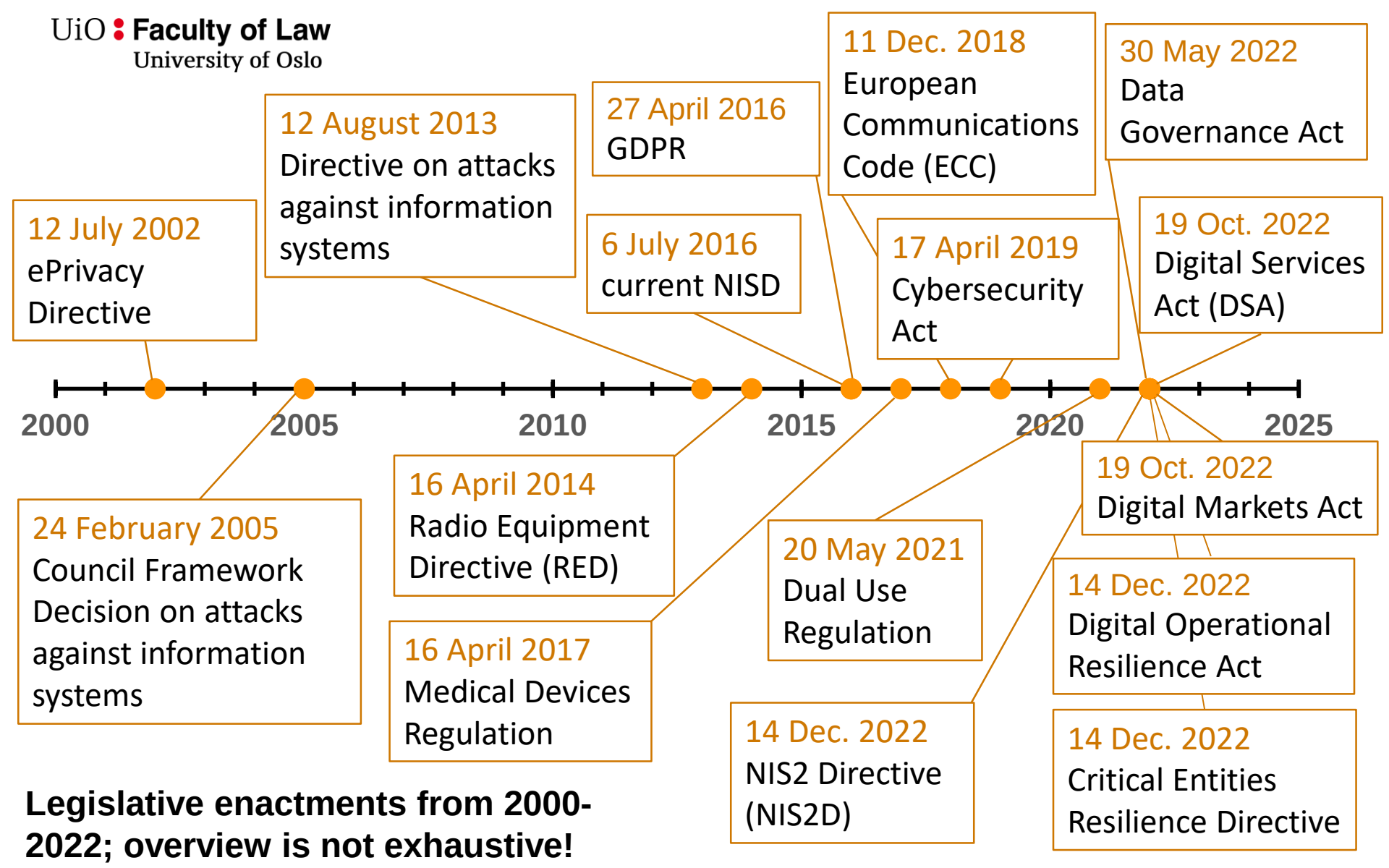
31 March 1992
Council decision 92/242/EEC in the field of security of information systems

15 December 1997
Telecommunications Privacy Directive 97/66/EC

24 October 1995
Data Protection Directive 95/46/EC

Legislative enactments from 1980-2000

UiO : Faculty of Law
University of Oslo



Legislative enactments from 2000-2022; overview is not exhaustive!

+ EU ‘primary’ law on security of personal data

- Arts 7 and 8 CFREU (and, indirectly, Art 8 ECHR)
- ECtHR: *I v Finland* (2008)
  - need for ‘practical and effective protection to exclude any possibility of unauthorised access’ (para. 47)
- CJEU: *Digital Rights Ireland* (2014)
  - ‘Member States are to ensure that appropriate technical and organisational measures are adopted against accidental or unlawful destruction, accidental loss or alteration of the data’ (para. 40)

+ EU cybersec law in the pipeline

- proposed Artificial Intelligence Act (AIA)
- proposed European Health Data Space Regulation (EHDS)
- proposed Cyber Resilience Act (CRA)
- proposed Data Act
- proposed Chips Act (CA)
- proposed Cyber Solidarity Act (CSA)

+ lots of ‘soft’ law

For example:

- EU Policy on Cyber Defence (2022)
- Strategic Compass for Security and Defence (2022)
- EU's Cybersecurity Strategy for the Digital Decade (2020)
- ENISA guidelines and certification system

General trends

- Increasing regulatory density + tempo
- Hybrid regulatory strategies
  - C&C;
  - meta-regulation;
  - design-based regulation etc.
- All-hazards approach
  - Safety + security + …

General trends [2]

- Increasing use of horizontal (as opposed to vertical) regulation
- Synthesis/marriage of various sectoral areas
  - Product safety law + health law + dp law etc.
- Ever greater procedural intricacy

General trends [3]

- Increasing design focus
  - Security by design (and by default) = fully fledged principle (see Bygrave (2022))
- Increased use of generic functional requirements rooted in ‘state of the art’
- Increasing focus on ‘resilience’

Strengths

- Greater awareness of (potential for) regulatory failure
- Greater awareness that security is iterative
- Greater in-built flexibility and agility in the rules, leveraging off engineering standards
- Resilience-focused ideals coming to the fore

Resilience rules!

Resilience has become a ‘quasi-universal answer to problems of security and governance, from climate change to children’s education, from indigenous history to disaster response, and from development to terrorism’

- Claudia Aradau (2014)

Increasing conceptual coherence?

EU regulatory policy on cybersecurity has developed without a ‘coherent understanding at the EU level about how to define “security”, and how its underlying values operate, relate or should be interpreted’, a state of affairs that ‘has allowed powerful actors to paint communications security any color [sic] they like’.

- Axel Arnbak (2016)

Resilience ↔ cybersecurity [1]

- GDPR treats ‘resilience’ as property of ‘security’
  - see Art. 32(1)(b) (‘the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services’); Art. 32(1)(c) (‘the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident’)

Resilience ↔ cybersecurity [2]

- NISD omits ‘resilience’ from definition of ‘security’ (or does it?)
  - security = ‘the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems’
  - does resistance = resilience?

Resilience ↔ cybersecurity [3]

- CERD treats security as property of resilience
  - Art. 2(2): ‘resilience’ = ‘the ability to prevent, resist, mitigate, absorb, accommodate to [sic] and recover from an incident that disrupts or has the potential to disrupt the operations of a critical entity’

And so what?

Resilience is ‘a powerful concept but … sufficiently ambiguous that it can become counterproductive if used carelessly’

– Benoît Dupont (2019)

Other points of muddle/confusion

- What = lex superior, lex generalis, lex spesialis?
- What = ‘state of the art’?
- What = hard law; what = soft law?

‘Where have all the judges gone?’

- Very little case law
- Soft law + RA decision making dominate
- Reliance on slippery concepts
  - e.g. ‘state of the art’, ‘appropriate’, ‘reasonable’
- More ‘grey-box decision making’ (Bygrave (2022))?

Proportionality rules (again)

- ‘appropriate’ measures in light of contextual factors
  - See e.g. Art. 32 GDPR
- Security = result of best reasonable effort
  - ‘an obligation of means’ (not ‘result’) (van Alsenoy 2016); but what means and how far?
- Cf. Case C-340/21, *VB v Natsionalna agentsia za prihodite* (pending)

References

- C. Aradau, 'The promise of security: resilience, surprise and epistemic politics' (2014) 2(2) *Resilience* 73 https://doi.org/10.1080/21693293.2014.914765.
- A.M. Arnbak, *Securing Private Communications: Protecting Private Communications Security in EU Law – Fundamental Rights, Functional Value Chains and Market Incentives* (Wolters Kluwer 2016).
- L.A. Bygrave, 'Machine Learning, Cognitive Sovereignty and Data Protection Rights with Respect to Automated Decisions' in Ienca et al (eds), *The Cambridge Handbook of Information Technology, Life Sciences and Human Rights* (2022) chapter 13 https://doi.org/10.1017/9781108775038.016.
- L.A. Bygrave, 'Security by Design: Aspirations and Regulatory Realities' (2021) 8(3) *Oslo Law Review* 126 https://www.idunn.no/doi/epdf/10.18261/olr.8.3.2.
- B. Dupont, 'The cyber-resilience of financial institutions: significance and applicability' (2019) 5(1) *Journal of Cybersecurity* 1 https://doi.org/10.1093/cybsec/tyz013.
- H.W.J. Rittel and M.M. Webber, 'Dilemmas in a General Theory of Planning' (1973) 4 *Policy Sciences* 155 https://doi.org/10.1007/BF01405730.