Hertie School

Shifting Narratives and Regulatory Principles in EU Data Policy: From Market Liberalization to Risk Governance and Data Maximisation

Risikonarrative im Feld Privacy, Surveillance und Datenschutz

Simona Stockreiter, PhD researcher Hertie School

- **Topic:** Analysis of the evolution of the "**regulatory principles**", "**regulatory instruments**" and "**risk narratives**" of **EU data policy** over the last 30 years

- **Research Questions:**

- ***How does EU legislation deal with the growing risks in the era of "big data and hyper-connectivity"?***
- ***How are regulatory principles and regulatory instruments changing, and what influence does this have on the perception and narratives of risk in a society?***

- **Method**: Qualitative content analysis of relevant legal texts, European Commission Strategies, Expert Interviews with Senior Officials and Experts

Phase I: Data Protection Directive (1995):

- ❖ Constituted the foundational legal instrument for data protection within the EU
- ❖ Served as a principle reference framework for data protection globally

- **two goals:**
- **1. Protection of Fundamental Rights: (Article 1(1))**
- **2. Enhance the Functioning of the Internal Market ☾ intends to remove barriers in order to facilitate cross-border data transfers within the EU (Article 1(2))**

Regulatory Principles:

- **Transparency :** data subject‘s right to information, right to access
- **Individual Data Control:** Right to request rectification, erasure, or blocking of data; Right not to be subject to decisions based solely on automated processing; Processing of personal data must be based (under certain conditions) on consent of the data subject

❖ **Primary goal:** harmonization of national legislation, **facilitate cross-border data flows within the single market**

☾ **No genuine balance between market-oriented focus and fundamental rights objective**

Normative Foundation:

- Period of Deregulation and Market Liberalisation *(Interview 1, Senior Official)*
- "You don't have to do anything; the delicate plant that is the internet needs time to grow first" *(Interview 2, Senior Official)*

Risk Narrative:

- Fear that the state is using data for totalitarian purposes *(Interview 1, Senior Official)*
- Fostering citizens' **trust as a prerequisite for market growth** *(Interview 3, Expert EDRi)*

2002 ePrivacy Directive:

- Introduced **sector-specific provisions** tailored to the unique characteristics of the digital communications environment

- **Reinforces principle of data control**: consent requirements for *tracking cookies*, *processing of location data*, *processing of personal data for marketing purposes*, *unsolicited communications* (e.g. marketing emails)
- **Reinforces principle of transparency:** *obligation to inform data subjects of data breaches*

- Focus on building **trust**: "**a high level of trust is essential for the effective functioning of the data-driven economy**" *(Recitals)*

Phase II: GDPR (2016)

- **two goals:**

- Article 1(2)GDPR: "***The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data***."

- Article 1(3) GDPR: "***The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data***."

Regulatory Principles:

- **Individual Data Control & Autonomy:** "**right to be forgotten**", **right to data portability; Strengthening of right not to be subject of decisions based solely on automated processing, including profiling:** right to obtain **human intervention,** right to **express their point of view,** right to **contest the decision;**
- **New individual right to compel action by supervisory authorities**; **Right to lodge a complaint** if authorities fail to respond or act; **Right to initiate civil proceedings** directly against data controllers.

- **Transparency:** New obligations for "**transparent information and communication**" *(**infos must be given in clear and plain language**)*; Data controllers are required to **maintain detailed records of data processing activities** *(-> planned to be weakened, reduced only to "high risk" processing under the GDPR "simplification proposal")*
- **Accountability:**
  - Principles of **data protection by design and by default** *(embedding privacy measures into systems and processes from the outset*);
  - **Data Protection Impact Assessments** (DPIAs) for high-risk data processing activities
  - **Obligatory designation of Data Protection Officer** (DPO) in certain cases
  - **Controllers must not only meet the requirements of the law but they must also demonstrate their compliance with the regulation**.
  - **Reversal of burden of proof in favour of data subjects** *(data subject must not proof the precise nature of legal violation by controller)*

Regulatory Instruments:

- **Risk-based approach: Regulatory Impact Assessments** ☾ 1. Data controllers must carry out "objective assessment" on whether data processing activity is high risk; 2. if high risk: they must implement appropriate mitigation meausures and supervisory authority must be notified; data breach notifications (only when data breach is likely to result in high risk)

à Enhances **regulatory flexibility (no one-size-fits-all approach**), efficiency, accountability, "competitiveness tool"

à Assigns **primary responsibility to data controllers**

- Strong **rights-based approach**: foundation in constitutional values (Article 8 Charter, Article 16 TFEU)

"***The risk-based approach can help prioritize resources, but it sits uneasily with a rights-based framework. Risk assessments often shift responsibility into controllers and can lead to superficial compliance exercises. In contrast, the rights-based approach demands strict observance regardless of risk levels***." (Interview 3,)

- **Expanded powers of supervisory authorities**, harmonized fines (€20 Mio/4% of global annual turnover)

Risk narratives:

- "the focus is on harm to individual rights and freedoms" *(Interview 3, Expert EDRi)*
- Due to rights-based approach:

➢ "***The risk in the GDPR was very subjective, it was linked to how the data subject would understand this risk and therefore all the emphasis was the possibility for the data subjects to exercise their rights, irrespective of any other consideration. The data subject is the ultimate assessor of the risk.***" *(Interview 1, Senior Official)*

➢ Focus on **individual autonomy**, "**the citizen as a holder of fundamental rights**", shifting **responsability** onto the individual

Phase II: "Counter-movement" Sectoral Regulation

- **Regulation on the Free Flow of non-personal Data (2018), Open Data Directive (2019), Payment Services Directive (2015):**
- Objectives: facilitate the free flow of non-personal-/public sector-/financial data across the EU, foster competitiveness & data-driven innovation
- Regulatory principles: **openness ("open data")**, **transparency** (recommended codes of conduct, public registers), **efficiency**, **security**
- Tensions: **partly conflicting with GDPR principle of individual data control**
- Risk Narratives: focus on **security risks**, goal: enhance **trust** ☾ of MS and private companies in the internal data market, "**neo-liberal counter-movement**" (Interview 2, Senior Official)

Phase III: Data Governance Act

- Horizontal regime for the **re-use of certain categories of protected data held by public sector bodies**
- Provision of "**data intermediation services**": "new ecosystem" to facilitate the connection between dater subjects and data users (supply & demand), "neutral **data marketplaces**" (handle personal data & commercially confidential data)
- Data altruism organisations: Concept of **data altruism** for the "**general, public interest**"
- Goal: **borderless digital internal market, (**"make as much data as possible available for sharing"), " "**it's really about opening up markets**" (Interview 4, Senior Official), **competitiveness ☾ Europe's position in the global data economy**

à Principles: **openness** (data portability), **transparency, efficiency, security**

à Instruments: risk-based approach

à Normative Background and Risk narrative: data as a resource, data maximization, "**rights are implicitly dispensable**", (Interview 2, Senior Offical), "**risks are framed as barriers to innovation and data reuse**" (Interview 3, EDRi)

à Problem: Data organisations decide to whom data is transfered; there are **no general guidelines on data anonymisation**

Phase III: Data Act

Hertie School

- Granting data subjects access to (industrial and IoT) **data generated by the use of products or services**, which is held by the data holder (manufacturer).
- Focus on **B2B data sharing**
- Goal: **data driven innovation**, **turn EU into a global leader for the data-agile economy**, **user empowerment**
- Principles: **fairness** in the data economy ("I control the data on my devices"), **transparency, efficiency**, **security, trust**

Conclusion:

à "***The DA and the DGA shift the paradigm towards data maximization to serve industrial and competitiveness goals. This risks undermining GDPR principles of purpose limitation, data minimization and individual control as well as the ePrivacy directive***."
(Interview 3, EDRi)

à **Two interviewees warn that the GDPR's rights-based approach might be undermined by pushing a risk-based or market-oriented rationale for data governance.**

Phase III: AI Act

❖ **Main Goals:**

- **Protection from physical** (e.g. AI cars crashing), **individual** (e.g. predictive policing), **collective** (e.g. systematized bias), **societal harms** (e.g. emotion recognition in automated hiring systems) + **supporting innovation and development of human-centric AI.**

Risk-based approach:

- **Prohibitions**: China-style social credit scoring, 'real-time' remote biometric identification systems,..
- **High-risk**: clear potential risks which are nonetheless deemed manageable: *Law enforcement, Administration of justice and democratic processes, Education, Employment and workers management, Healthcare, Management and operation of critical infrastructure, Access to and enjoyment of essential private services and public services and benefits, Migration, Asylum and border control management*

  ➢ Example Employment: automated hiring system (☾ emotion recognition: tells whether you are happy when you are doing your task)

  Obligations: **wide range of "high-risk" AI systems would be authorized, but subject to a set of requirements and obligations to gain access to the EU market**.

  - Example: **high quality training data set** ☾ data must be relevant, representative, free of errors
  - Ensure **human oversight** when using of AI system,..

Regulatory Instruments:

Hertie School

❖ **Pure market surveillance, as in previous regulations for technical safety of products**

❖ **No enforcement options for citizens as in the GDPR**

❖ **Range of Self-Assessments:**

- **Conformity assessments** (assessment of manufacturers / conformity assessment bodies whether the products confirm with the product safety standards)
- **Assessments concerning high-risk classifications** (*self-assessment* whether AI system is not high-risk)
- **Fundamental rights impact assessments** (requirement for deployers acting in the context of public service provision)
- **GPAI risk assessments**: (GPAI models with systemic risks are required to i.a. self-assess and mitigate potential systemic risks)

Hertie School

Regulatory Principles:

- (Product) Safety, Efficiency, Transparency, Openness
- Partly conflicting with GDPR principles of data control & data minimization (e.g. remote biometric identification, workplace surveillance)

Risk Narratives:

- Focus on **systemic risks**, though **operationalist in ways that legitimise many harmful practices** *(Interview 3, Expert EDRi)*
- "*This approach proposes the idea that as long as you can mitigate some **technical risks**, then the problems are solved…as long as you place some kind of technical means of debiasing, human oversight measures etc. into the system, then everything seems fine. But we should be more critical about what kind of systems we actually accept as maybe a society to be used.*" *(Interview 12, Mher Hakobyan, Advocacy Advisor on AI Regulation at Amnesty International)*
- ***"**The focus is on **product criticism** and **risk management** rather than on the democratic shaping of our future" (Interview 2, Senior Official)*
- *"Focus has been **shifted away from the subjective perspective of the data subject to the product itself.** So, its not so much what you or I or the data subject or user may think about it." (Interview 1, Senior Official)*

Regulatory Framework	Phase I: Data Protection Directive, ePrivacy Directive	Phase II: GDPR	Phase II: Regulation on the Free Flow of non-personal Data , Open Data Directive, Payment Services Directive	Phase III: Data Act & Data Governance Act	Phase III: AI Act
Regulatory principles	- Transparency - Individual data control	- Transparency - Data control and individual autonomy - Accountability	- Openness - Transparency - Efficiency - Security	- Openness - Transparency - Efficiency - Security	- (Product) Safety - Transparency - Efficiency - Openness
Regulatory instruments	- Directive - no harmonized enforcement	- Regulation - Harmonized enforcement - **Rights-based approach** - Risk-based approach	- **Risk-based approach** - Technical standards	- Regulation - **Risk-based approach**	- **Risk-based approach** - **Market surveillance** - Self-Assessments - **Technical Standards**
Regulatory objective	- **Market opening**	- **Stronger tension between fundamental rights protection and market-making objectives** - Importance of data control	- Foster competitiveness - Data driven innovation - **Market opening**	- **Market opening** - Data driven innovation - EU Data Sovereignty	- Protection from **systemic harms** - Innovation
Risk narrative	- **Protection from state intervention** - **Building trust**	- **Focus on harm to individual rights & freedoms** - **"subjective“ risk** - **Individual empowerment**	- **Focus on security risks** - **Risks as barriers to innovation** - **Building trust**	- **Focus on security risks** - **Risks as barriers to innovation** - **Building trust**	- Targets **systemic risks** - Focus on **technical risks** - **Product criticism** - **Risk management**
Regulatory narrative	- Data protection as a technical subject - Economic discourse	- New focus on risks to fundamental right of data protection - highly salient political issue (Snowden revelations) - tech companies as “enablers of sate surveillance” - GDPR as “the golden	- “neo-liberal counter-movement”	- Industrial policy - Europe’s position in the global data economy	- “It's more about risk management than responsibility for the future.“ - Individual, collective, systemic harms