idec
Instituto Brasileiro de Defesa do Consumidor

OS MITOS DA REGULAÇÃO NO DEBATE DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Instituto Brasileiro de Defesa do Consumidor
Rafael A. F. Zanatta

Seminário conjunto realizado pelo Comissão de Ciência e Tecnologia e Comissão Especial do Projeto de Lei 4060/12 e 5276/16

Brasília, 22 de maio de 2018

2018: ano da proteção de dados?

- Oficinas, eventos públicos e campanhas
- 15 de março: lançamento da campanha “Chega de Desproteção”
- Ampliação para ação “Sorria, você está sendo rastreado”
- Atuação com a Coalizão Direitos na Rede

Dados pessoais não são mercadoria

Nossas informações não podem ser registradas e usadas para além daquilo que autorizamos inicialmente. Precisamos ter disponíveis formas de saber quais dados são retidos e a qualquer momento desistir da permissão. Na prática, defendemos uma legislação em que:

- ✓ Pessoas possam controlar todo o fluxo de dados gerados por elas
- ✓ Empresas respeitem princípios éticos que regulem a forma como tratam os dados
- ✓ Empresas e governos se responsabilizem quanto ao vazamento de dados, sujeitos a cobrir indenização em casos de uso indevido de nossas informações

E tem mais: para que a lei funcione, é preciso que haja uma autoridade pública que fiscalize os direitos digitais para evitar mais violações e abusos.

O Idec luta por essa proposta junto a outras 20 organizações civis que formam a Coalizão Direitos na Rede.

idec
Instituto Brasileiro de Defesa do Consumidor

Regulação e defesa de direitos

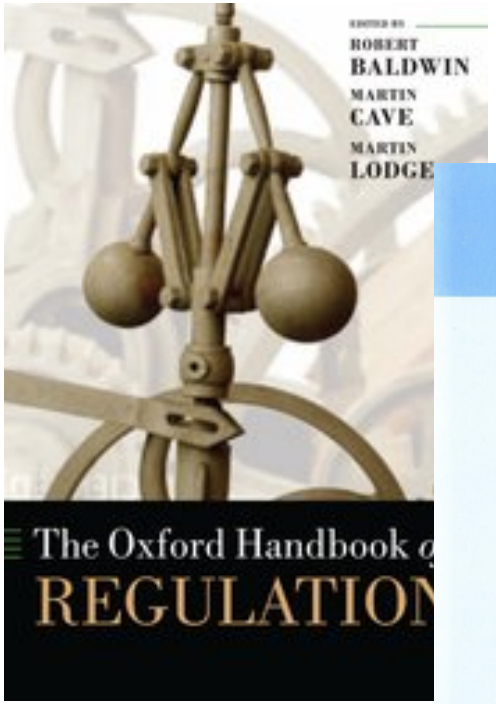
"Acesso liberado? Só com a minha anuência consciente; do contrário, é pura pilhagem!"

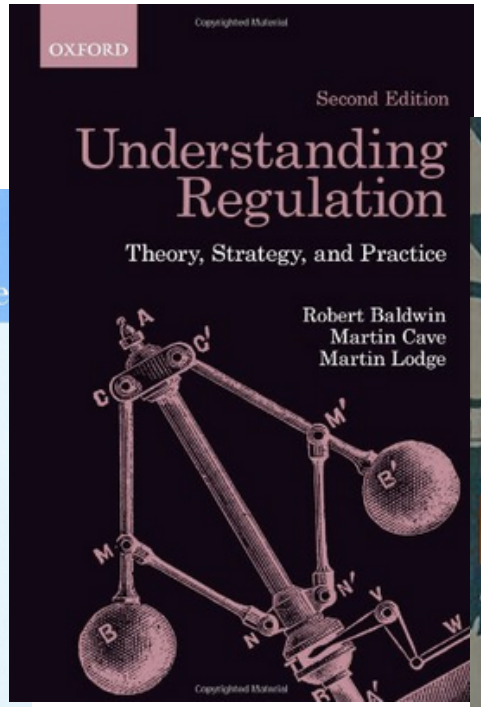
MARIO SERGIO CORTELLA
Escritor, filósofo e professor

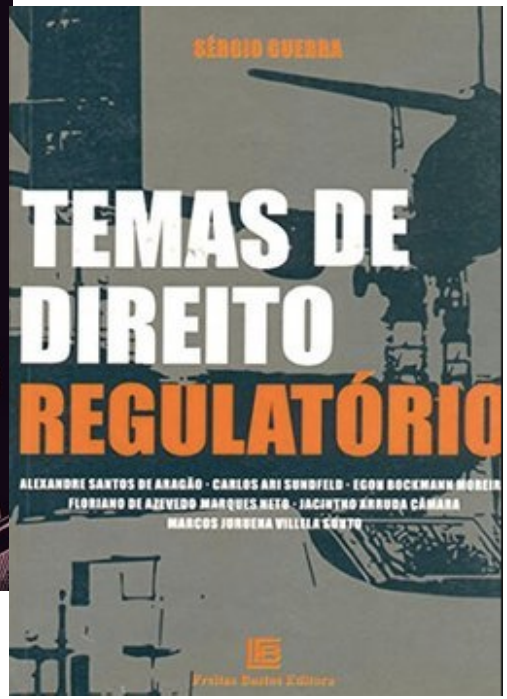
Por que precisamos de regulação?

- Não se trata somente de falhas de mercado.
- Regulação também se constrói a partir de uma abordagem baseada em direitos.
- É preciso clareza sobre o que regular e por que regular.
- A regulação de mercados objetiva a modificação de determinados comportamentos e se dá por um complexo empreendimento.

Estudos de regulação







5 mitos sobre regulação e proteção de dados pessoais

idec
Instituto Brasileiro de Defesa do Consumidor

“Os EUA conseguiram uma forte indústria de dados pela baixa regulação”

Cenário nos EUA

- Mais de 2.000 normas jurídicas sobre privacy.
- Forte atuação da Federal Trade Commission na criação de uma “privacy common law”.
- Setores de crédito e de saúde fortemente regulados com normas setoriais.
- Tradição regulatória desde o New Deal (regulatory agencies) e multas pesadas com possibilidade de “sanções punitivas” (punitive damages).

“A regulação pode acabar com a inovação e o futuro da economia digital no Brasil”

O exemplo da Comissão Europeia

- Estratégia de transformação digital tem como componente a proteção de dados pessoais.
- Combinação entre fomento à inovação (segurança jurídica) e garantia dos direitos fundamentais dos cidadãos.
- Preocupação com questões sistêmicas maiores: política fiscal, acesso a recursos para inovação, compartilhamento de conhecimento e capacitação.

“A regulação europeia de dados pessoais é um intervencionismo estatal prejudicial”

Como funciona a GDPR

- Afirmação de direitos dos titulares e adoção de mecanismos de mitigação de riscos coletivos.

- Atribuição de muitos novos papéis ao setor privado (*e.g.* elaboração dos "impact assessments" e definição dos códigos de conduta) e adoção de mecanismos de **co-regulação**.

- Possibilidade de liderança do setor privado no processo de co-regulação (organização de melhores práticas e incorporação de privacy by design).

“O Brasil possui regras suficientes e uma estrutura de defesa do consumidor que dá conta dos problemas atuais”

Cenário brasileiro

- A “colcha de retalhos” construída em diferentes legislações é tímida na definição de princípios de proteção de dados, direitos dos cidadãos e formas de mitigação de riscos. Há amplo consenso entre especialistas.

- A Secretaria Nacional do Consumidor (Senacon) sofre de problemas orçamentários, staff insuficiente e constantes trocas de coordenação.

- Situação brasileira é incomparável com a estadunidense e a experiência da FTC.

“A Lei de Dados Pessoais coloca muito poder na mão do Estado”

Regulação por autoridade independente

- Experiência internacional revela independência funcional e formal para autoridades de proteção de dados pessoais.

- O regulador monitora experiências do setor privado e as práticas do setor público. O olhar para possíveis práticas ilegais/abusivas por parte do Estado é tão grande quanto o monitoramento do setor privado.

- Autonomia: regulador precisa de mandato, independência financeira e possibilidade de atuação sem interferências diretas.


Identify and prepare
Design and Implement
Operate and Secure
Current state assessment and gap analysis
Map data flows across products and services
Establish the legal basis for processing personal data
Privacy risk assessment across products and services
Governance structures to achieve future state operating model
Implement privacy controls to reduce risk to acceptable levels
Map information assets to explicit consent requirements
Ownership of personal data aligned to the business model
Appoint a DPO and regular reporting to the board
Audit schedule to ensure compliance and controls are transitioned to BAU
Regular consent audits in the business units
Full information lifecycle management

EY (2018)

Para onde podemos ir?

- Afirmação de direitos, privacy by design, maior enfoque em controle de riscos e atribuição de obrigações ao setor privado.
- Co-regulação: possibilidade de experimentação, introdução de melhores práticas e retroalimentação.
- Criação de autoridade independente com autonomia funcional e financeira, expertise técnica e capacidade de utilização de diferentes instrumentos regulatórios.
- Necessidade de poderes de definição técnica (situações de alto risco que demandam avaliação de impacto com mais cuidado e detalhamento).

Estaremos mais próximos ou distantes da GDPR?

EU GENERAL DATA PROTECTION REGULATION

Enforcement starts on May 25th, 2018

Concerns organizations processing personal data of EU citizens

- **Increased Territorial Scope** (extra-territorial applicability)
- **Penalties**: fines of up to 4% of annual global turnover or €20 Million (highest of both)
- **Consent**: clear consent to process data (and ability to withdraw)
- **Breach notification duty**: within 72 hours of having become aware of it (if risk)

http://www.eugdpr.org/the-regulation.html

- **Right to access**: controller must answer whether personal data are processed; why + where; copy
- **The right to be forgotten**: Data Erasure (conditions)
- **Data portability**: right to transmit personal data to another controller
- **Privacy by design**: from concept to legal requirement
- **Data Protection Officers**: staff member or external service provider

Summary of some key changes with GDPR

idec
Instituto Brasileiro de Defesa do Consumidor

www.idec.org.br/dadospessoais

www.idec.org.br/vocerastreado

www.direitosnarede.org.br

rafael.zanatta@idec.org.br