



Regulatory policies that may impact the DNS

André Gomes

26 April 2022

Table of contents

- About Cullen International
- Policy implications of technical decisions
- Technical implications of policy decisions
- Status in Latin America and the Caribbean

**We are an independent
regulatory intelligence
provider.**

who we are



Independent, impartial and active in **70 countries**, we help organizations see **the bigger picture** behind regulation and competition law in the **communications sector**.



who we are
in numbers

regulation
made simple

>35

Years of
Experience

70

Countries Covered

4x4

Covering
4 Sectors Across
4 Continents

>50

Team Members

>270

Clients
from

25

Different
Nationalities

90

Different
Countries

26

Different
Languages

Back to basics

The internet was built to share information:

- Efficient: shortest route
- Robust: independent networks

Series of technical
decisions



Brief History of the Internet

Transmission Control Protocol/Internet Protocol (TCP/IP)

“Four ground rules were critical to Kahn’s early thinking:

- Each distinct network would have to stand on its own and no internal changes could be required to any such network to connect it to the Internet.
- Communications would be on a best effort basis. If a packet didn’t make it to the final destination, it would shortly be **retransmitted** from the source.
- Black boxes would be used to connect the networks; these would later be called gateways and routers. There would be **no information retained** by the gateways about the **individual flows** of packets passing through them, thereby keeping them simple and avoiding complicated adaptation and recovery from various failure modes.
- There would be no global control at the operations level.”

Technical implications of policy decisions

Privacy

Harmful and
illegal content

Security and
resilience

Risk of
fragmentation

Privacy

- **DNS queries can reveal**
 - what websites an individual visits
 - meta data about other services
- **DNS should be public, but DNS transactions probably not**
- **Problem partly addressed by tools adopted by DNS resolvers**

GDPR

Harmful and illegal content

- Dynamic blocking injunction, incl. to DNS resolvers in some countries
- Injunction to some but not all providers
- Risk of over- and under-blocking

Security and resilience

- **Directive on the Security of Network and Information Systems (NIS2)**
 - “Essential” digital infrastructure: cloud computing, IXPs, DNS services, top level domain (TLD) name registries (main establishment in the EU)
 - Supervision may include: regular and targeted audits, on-site and off-site checks, request of information, and access to documents or evidence

Risk of fragmentation? The DNS4EU

- Free: DNS resolution, free parental control, compliance with EU rules
- Paid premium services for corporate users: for enhanced performance or security

What about Latin America and the Caribbean?



Thank you!

andre.gomes@cullen-international.com