0° minute: A First Look to Collateral Damages and Efficacy of the Italian Piracy Shield

Raffaele Sommese, Anna Sperotto, Antonio Prado,
Jeroen van der Ham, **Antonia Affinito**

UNIVERSITY OF TWENTE.

DACS

About me

Antonia Affinito

- Assistant Professor at Design and Analysis at Communication Systems (DACS) - EEMCS Faculty **at the University of Twente**
- **Research Interests**:
  - Cyber Threats Detection
  - Internet Measurements
  - Sustainable Internet

The platform

- Donated to AGCOM by SP Tech
- Copyright holders have access to insert “tickets”
  - They contain IP Addresses and/or FQDNs to block
- ISPs query the system, download the latest tickets and apply the filtering
  - This needs to be done in 30 minutes

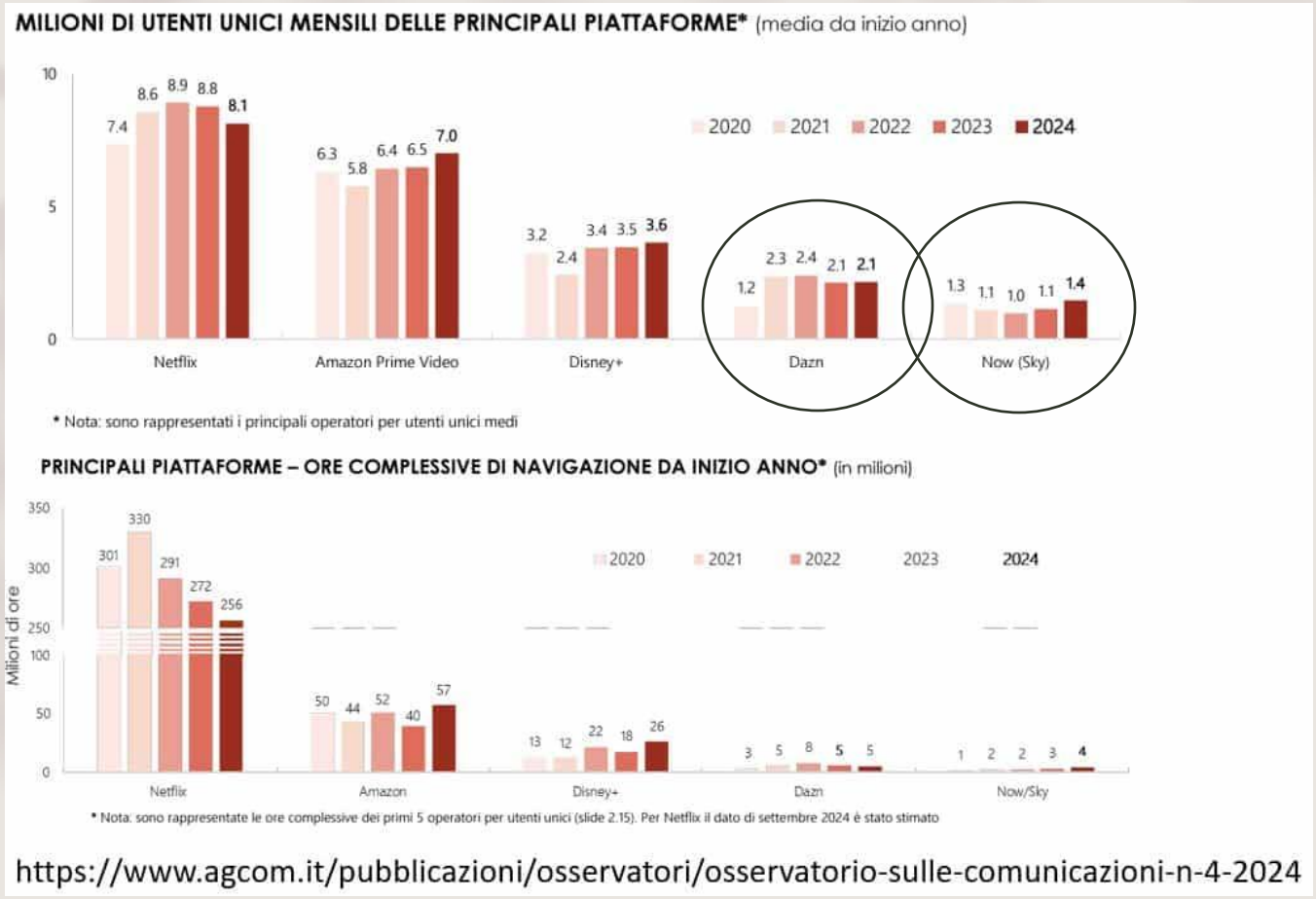
But what if they make a mistake? Can I complain?

...In very few cases

But there's no formal way!

Some mistakes down the road

- On 1st February 2024:
  - An IP address from **Cloudflare** made it into the list.
  - Tens of thousands of websites were unreachable for around 40 hours from Italy
- **Zenlayer** and **Imperva** also had some of their addresses make into the list
- At 18:56 on 19th of October, a copyright holder decided that **drive.usercontent.google.com** needed to be put on the list.
  - Block was removed at about 00:20 on 20th of October.
  - But for hours Google Drive was unreachable from Italy
  - Someone claimed this was due to streaming playlists hosted on Google Drive.



https://www.agcom.it/pubblicazioni/osservatori/osservatorio-sulle-comunicazioni-n-4-2024

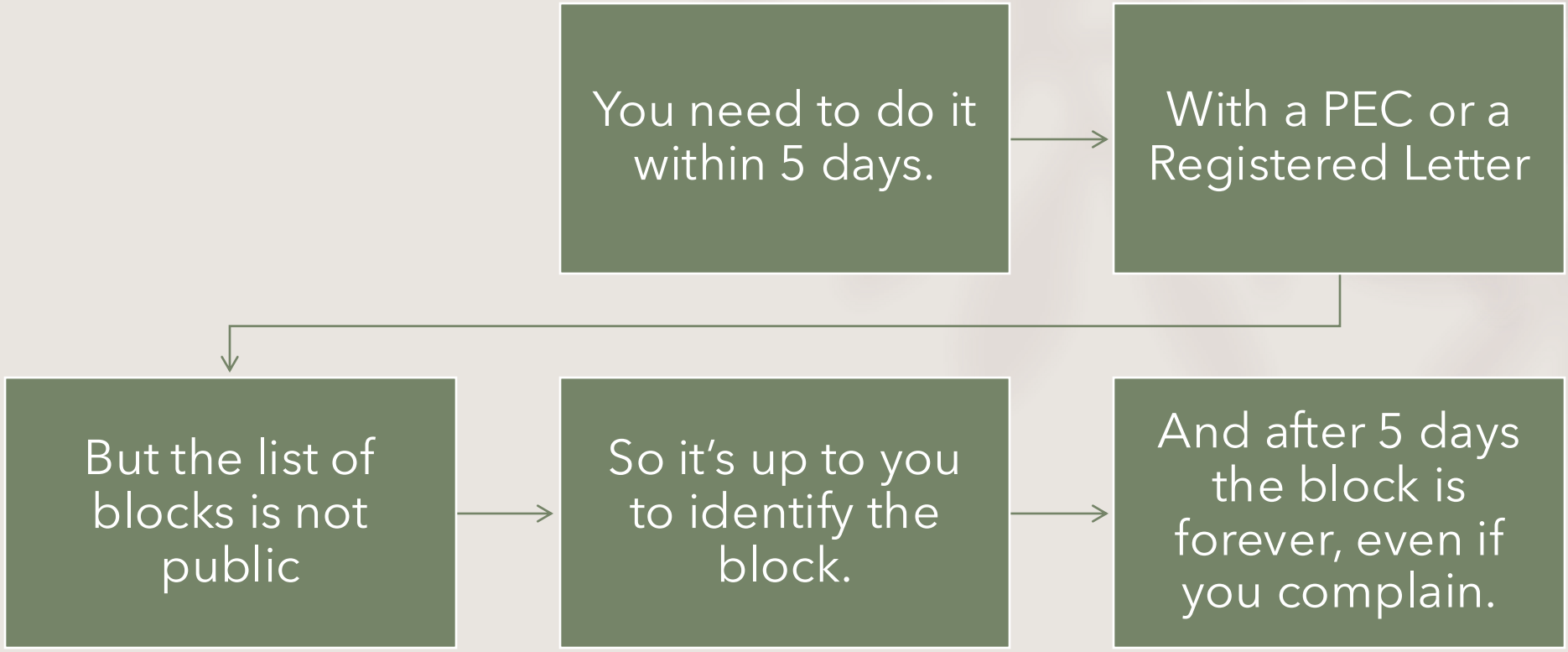
At least it worked right?

The number of users of **legal** streaming platform post piracy-shield in 2024 is the same of 2023

The new law (Oct 2024)

- IP addresses now need to be used **predominantly** for illegal activities
  - There is an official **unblock concept** now
- VPN and DNS providers are also subject to applying filtering
  - Independently of where they are located

OK, but at least I can complain now?



To summarize

- **Piracy Shield** was introduced in Italy in **2023** to allow copyright holders to request the **blocking of IP(v4) addresses and domain names** involved in illegal football streaming – within **30 minutes** of detection.
- In short:
  - **Unvetted blocking powers** granted to private entities
  - **No clear expiration** or review process for block orders
  - **Lack of transparency:** no public registry of blocked resources (not even under FOIA)
  - **Collateral damage** incidents affecting legitimate services (e.g., Google Drive, Cloudflare)

Reconstructing Transparency

The **absence of a public list** of blocked resources made assessing **collateral damage** nearly impossible.

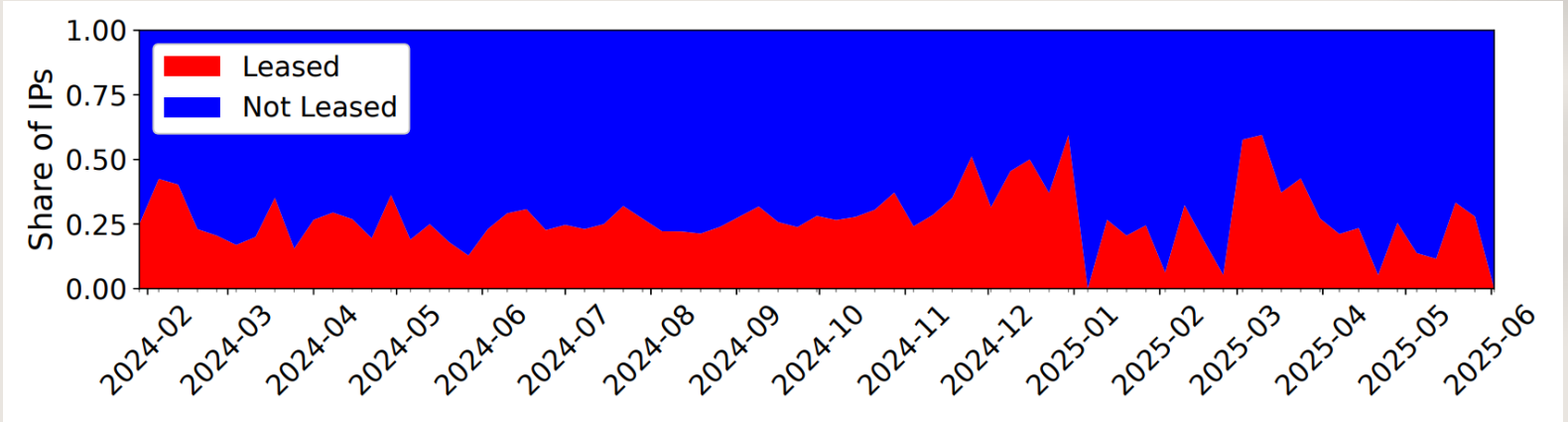
- To overcome this:
  - We used an **unverified leaked list** published on GitHub
  - We **validated entries** through the official AGCOM verification tool and the Infotech (an Italian ISP) website
  - Solving thousands of CAPTCHAs!

Pirates with an EU flag on the boat

Of the **10,918 blocked IPs** (across **2,134 /24s** and **262 ASNs**):

- **77%** geolocated within the **EU**, with **38% in the Netherlands**
- GZ Remittance alone hosted **>9.5%** of all blocked IPs, concentrated in **15 /24s**

Collateral Damage #1: IP Leasing



- We used Du et al. and Bernhard et al.'s methodology to identify leased prefixes.
- Out of 10,918 blocked IPs, 24% were **leased**.
- Streamers may exploit, consciously or not, the leased IP market, increasing the risk of **collateral damage** for legitimate businesses.
- **4%** of blocked IPs were leased out to new users *after* the block was implemented.
  - With the help of IPXO, we identified **250 IPs** as re-leased to different companies after the blocking date.
- Unsuspecting businesses are acquiring blocked and unusable resources on the Italian Internet.

Collateral Damage #2: Shared Infrastructure

- We identified a total of 7,114 FQDNs collaterally damaged by Piracy Shield
  - Among these, 1,931 responded to HTTP or HTTPS requests.
  - We manually classified **510 non-streaming-related websites** and 617 streaming-related.
  - 131 blocked IP addresses are responsible for 508 cases of collateral blocking.
  - Most legitimate affected websites were in French, Spanish, and German, and **9 in Italian.**
  - One notable case involves **19** legitimate Albanian websites hosted on **a single IP** address assigned to WIIT Cloud. These sites are **still unreachable** from Italy.
- Looking at historical collateral blocking, we found that 7,742 FQDNs were impacted by collateral blocking, 665 of which still active and non–streaming-related.

Collateral Damage #4: Expired FQDNs

- 10% of the 18K still blocked FQDNs were **unresolvable**.
- Unresolvable FQDNs tend to have an **earlier blocking date**. Abandoned by streamers?
- Among the 24K **unblocked** FQDNs, 34% of them were **still resolvable**. Were they removed only based on insertion date?
- Based on RDAP data, 119 FQDNs were **re-registered** after the blocking date, indicating possible **collateral damage** due to the reuse of the names.

Do streamers evade the blocking?

- Piracy Shield blocks only IPv4 and FQDNs so far, leaving a **potential loophole** for IPv6.
- Using historical OpenINTEL data, we found:
  - 1,568 blocked FQDNs started **serving over IPv6.**
  - 5,259 FQDNs adopted at least one **new IP**, but only 1,220 of those were blocked afterwards.
- These patterns suggest that illegal streaming operators can evade the platform via IPv6 and IP migration.

Photo by iMattSmart on Unsplash

UNIVERSITY OF TWENTE.

Questions?

Antonia Affinito

a.affinito@utwente.nl

Full paper: