When Consent Becomes a Blind SpotPersonal Data Exploitation, Psychological Targeting and Its Impact on Democratic Integrity

Core question: what happens when data collected for advertising becomes useful for profiling, manipulation — or a hostile state?

Manuela Petrescu, UBB

Case study: Snoop investigation, published 9 September 2026

1.Dark patterns /collecting data without consent

Design choices that make the privacy-friendly or autonomous choice harder.

Nudging the interface

A bright “Accept all” button, hidden rejection, pre-selected options, repeated prompts, or confusing wording.

Sometimes accept is not given!!!

Why it matters

The interface can distort informed choice — especially when users are tired, rushed, or unable to understand the data ecosystem.

Exploits natural curiosity or interest.

The data consequence

A click can enable cookies, pixels, identifiers, fingerprinting and behavioural tracking that feed a larger profile.

Dark patterns are not “just bad UX”: they can affect privacy, autonomy, money and psychological well-being.

Thanks to Snoop article



Medic: „Dacă te dor articulațiile, elimină asta imediat din dietă.”



Venele inflamate vor dispărea în 7 zile și nu vă vor mai chinui, dacă...



Cantități mici de scaun și constipație permanentă? Descărcați...



Mănâncă asta înainte de culcare și vei pierde 23 kg în 3 săptămâni...

Screenshot from the website of România TV

2. From one click to a behavioural profile

The important unit is not one data point — it is the combination.



Visit a site

page + device

Tracking

pixel / cookie / fingerprint

Link identifiers

click IDs + technical signals

Infer interests

topics, habits, vulnerabilities

Target

ads, content, persuasion

The profile is more valuable than any single data point

Combined signals can reveal interests, habits and potential vulnerabilities — and make audiences easier to target.

Profiling can be used to analyse or predict preferences, behaviour or characteristics.

3. The Romanian case: what Snoop documented

Five months of technical monitoring of online advertising infrastructure.

100,000+

ads monitored

131

sites in Eastern Europe

1,145

pages analysed

79

Romanian publications reported as having run AdNow ads/trackers

How they checked

Captured ad code and browser traffic; decoded obfuscated code; analysed .HAR files to observe requests, pixels and click tracking.

What they reported

Tracking identifiers could persist across sites and were observed being sent to servers associated with AdNow infrastructure, including Russian infrastructure.

Why it matters

Snoop argues that such data can support profiling and become an instrument of surveillance or influence when accessible to authoritarian actors.

The investigation documents technical data flows and presents a security-risk argument; it does not prove that every tracked user was individually targeted in a hybrid operation.

Source: Snoop investigation • 9 Sep 2026

4. Romania, an isolated case or is all Europe at risk?

Poland

"A digital war with Russia is underway, and within this digital war lies a front of disinformation. On this disinformation front, there is a silent ally to the Russian bots and the Kremlin's GRU: social media platforms"-
Krzysztof Gawkowski Deputy Prime Minister and Minister of Digital Affairs of Poland – Reuters

France

In run-up to mass protests and riots, pro-Russian accounts amplified French anger, NGO finds

Exploits natural issues in each country

Italy

Moscow stoked weekend riots in Europe, Italy says – Telegraph UK

Moldova

Disinformation & Hybrid Operations: The Kremlin utilizes coordinated multi-language media networks (such as *Pravda*), AI-generated deepfakes, and secret training camps in the Balkans to organize anti-government protests and disrupt social cohesion. – Stratcom, closing TVs and Media, Parties outside the law, etc.

ALL Europe at risk?

https://www.reuters.com/technology/poland-says-social-media-firms-are-silent-ally-russia-threatens-fines-2026-10-21/?utm_source=chatgpt.com
https://www.france24.com/en/in-run-up-to-mass-protests-and-riots-pro-russian-accounts-amplified-french-anger-ngo-finds
https://www.telegraph.co.uk/world-news/2026/10/21/moscow-stoked-weekend-riots-in-europe-italy-says/
https://www.lowyinstitute.org/the-interpreter/how-russia-tried-manipulate-moldova-s-election-what-it-reveals

5. Recent Political and Corporate Figures (Post-2022 Ukraine Invasion) – we are at war?

- **Tatjana Ždanoka (Latvia):** An MEP from Latvia who was exposed by investigative journalists as a long-term asset working directly under handlers from the Russian Federal Security Service (FSB). [1]

- **Maximilian Krah (Germany):** A prominent politician for the Alternative for Germany (AfD) party who faced intense scrutiny and investigation after it was revealed he was close to pro-Russian oligarchs and that his staff gave a suspected Russian spy access to the European Parliament. [1]

- **August Hanning (Germany):** In a major intelligence scandal, the former head of Germany's Federal Intelligence Service (BND) from 1998 to 2005 was arrested on suspicion of espionage and treason. He allegedly obtained classified files via a current BND employee, Manfred D., in exchange for money. [1]5.

6. What can we do with limited resources?

Focus on leverage points rather than trying to educate everyone about everything.

1 — Educate the population

Create a 60-second “data literacy” message:

- Don’t click by reflex
- Check cookie choices
- Limit unnecessary permissions
- Use privacy tools / ad blockers
- Pause before sharing or reacting to personalised outrage

Requires resources, large campaines, hard to sustain to have a relevant impact.

2 — Equip decision-makers

Give public officials, schools, NGOs and journalists a short checklist:

- Who receives the data?
- What identifiers are used?
- Is consent meaningful?
- Where are servers / processors?
- Could the dataset enable profiling?

The only effective safeguard remains the use of an ad blocker (snoop).

3 — Take SNOOP methods and apply in other countries

Action:

- requires expertise and
- human resourses
- media – for using the data to change something
- periodic spot checks of high-reach sites / other manipulation methods

The objective is not perfect privacy. It is to reduce the easiest paths from data collection → profiling → manipulation.

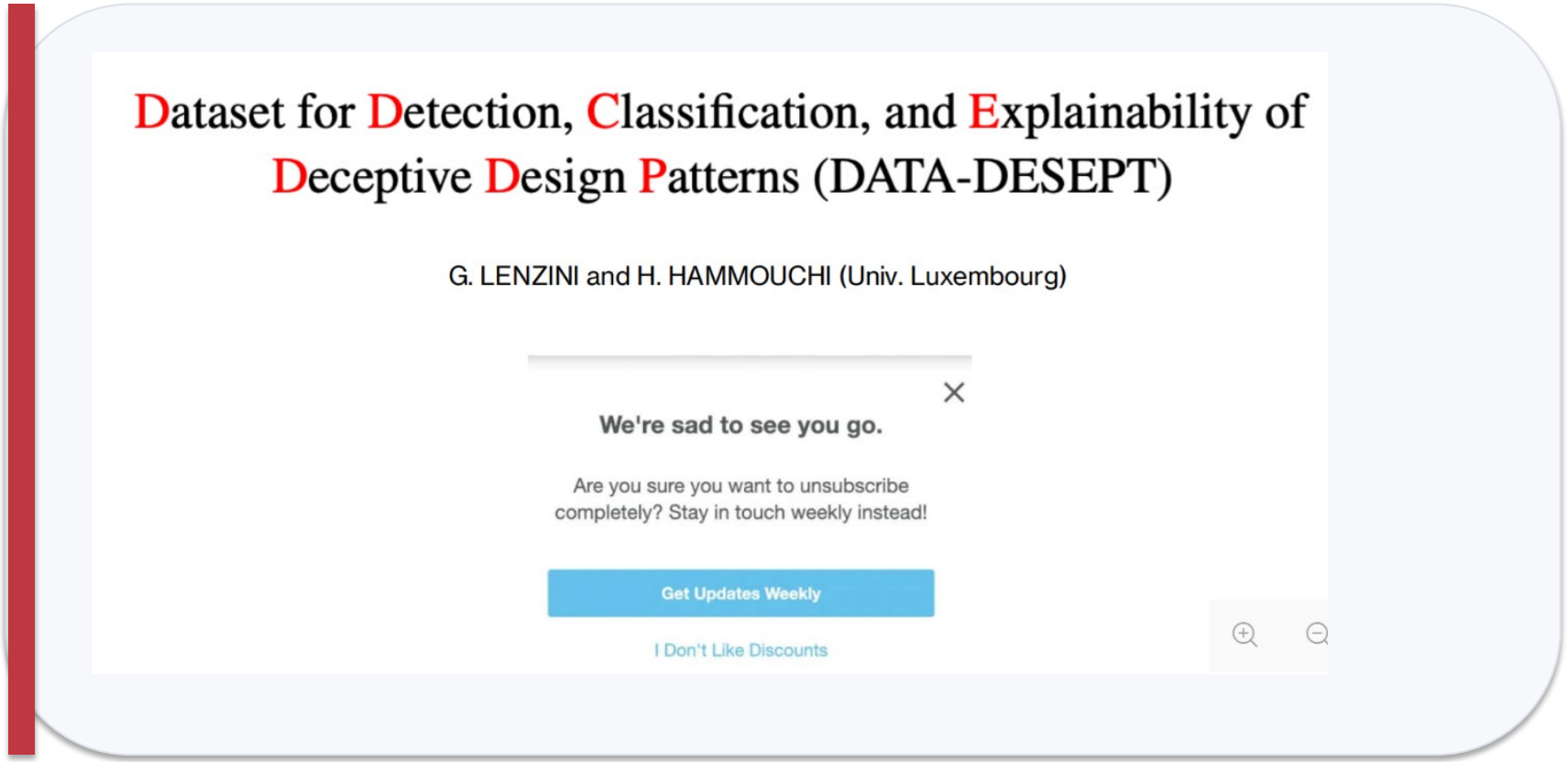
5. We are at war - economically?

Russia secretly financed Alaska gas project - Almost the entire management team of the US$25 billion US gas project Polar Train LNG has left the company following allegations of undisclosed financing and control by Russia's Novatek.
Financial times - https://www.ft.com/content/e9cfbfbb-e65a-4303-aebb-20d59319ef1b, 24 October 2026

On **October 13, in France**, 400 supermarkets were brought to a standstill after hackers breached their refrigeration software. The attackers raised the temperature inside the refrigerators to as high as 50 degrees Celsius. They caused fires and destroyed millions of euros' worth of fresh food.
European Commissioner for Agriculture and Food Christophe Hansen stated that food security has become a direct target and that the use of food as a weapon is a reality.

7.University Efforts

A combined effort and raising awareness – we could all benefit from



7. The takeaway

Personal data is becoming a strategic resource.

1

1. Consent must be real

A banner is not meaningful consent if the interface manipulates the choice — or if data flows after refusal.

2

2. Profiling changes the risk

The combination of identifiers and behaviour can reveal interests, habits and vulnerabilities.

3

3. Awareness is a security measure

With limited resources, target high-leverage audiences: educators, journalists, public institutions and decision-makers.

“If data can identify people, it can also identify who is easiest to persuade.”

Source: Snoop (2026). Supporting context: EU data-protection framework; OECD on dark commercial patterns; EU/EEAS materials on hybrid threats.