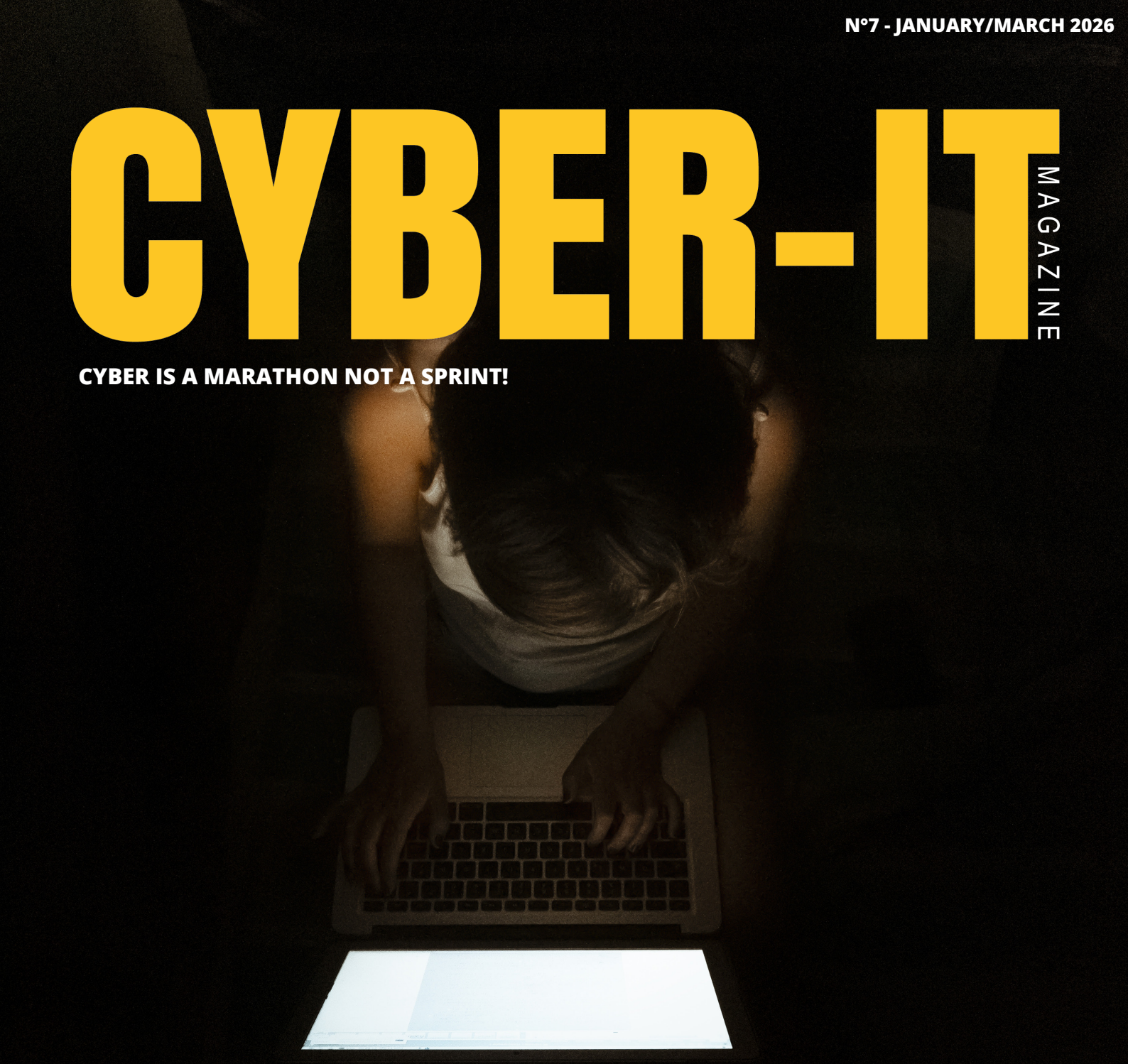
N°7 - JANUARY/MARCH 2026

CYBER-IT MAGAZINE

CYBER IS A MARATHON NOT A SPRINT!



SPECIAL REPORT

PERSONAL DATA

How much is it worth,
and who is competing for it?

Any questions? Please contact our team:
cyberit.magazine@gmail.com

EDITO

In light of the data breaches that have emerged in recent months, it became clear that personal data had to be the focus of this issue. It is hard not to feel a sense of concern when we consider how freely our information can circulate and how easily it may end up in the hands of malicious actors.

However, it would be unrealistic to overlook our own responsibility in this exposure. Through inattention or habit, we often accept terms and conditions without reading them, or share personal information by taking part in online games or filling out questionnaires, sometimes without fully understanding the consequences.

This investigation also shows how the tools we rely on every day, like our smartphones, can turn into powerful means of surveillance. We examine those who collect and exploit this data, and who have turned personal information into a particularly lucrative business.

Health data plays a central role in this report as well. Several were explored, testimonies gathered, and key questions raised all the way to the French National Assembly.

Any discussion of data leaks would be incomplete without addressing the darker side of the internet. We looked into these shadow spaces where large amounts of sensitive information are exchanged and concentrated.

Finally, the National Cyber Unit of the French Gendarmerie invited us in, offering a closer look to its mission and the realities of its day-to-day investigations.

Enjoy and see you very soon!

ARNAUD LEROY & MAËVA ASTORGA

SOMMAIRE

INTRO

PERSONAL DATA

Florian Bayard
Journaliste at 01Net

JWith more than eight years of experience as a journalist, Florian has explored a broad range of topics, from consumer technologies to the fast-evolving world of cryptocurrencies.

Over time, he has developed a strong expertise in analyzing digital practices and their impact on society. Now part of the editorial team at 01net, he focuses on making cybersecurity challenges understandable to a broad audience, breaking down online threats in a clear and educational way to help readers better understand the risks facing both the internet and its users.

The Rising Threat of Data Breaches in France

Data breaches continue to dominate headlines in France. Companies, telecom operators, government agencies are all being targeted by cybercriminals in search of information about French citizens. This article explores a growing digital threat.

Based on my experience as a cybersecurity journalist at 01net, this article offers a clear and accessible look at data breaches. In recent years, a significant part of my work has involved tracking data breaches across France, including leaks circulating on the dark web.

But what exactly is “data”?

Personal data refers to any information linked to an internet user. At its most basic level, this includes contact details such as your last name, first name, email address, phone number or postal address.

In many cases, these details are combined with far more sensitive information: banking data (credit card details or IBANs), passwords, medical history, or even biometric data. Biometric data includes identifiers such as fingerprints, facial features or iris scans. When combined, all these data make it possible to build an extremely precise digital profile, a detailed portrait of who you are.

Who holds your data ?

Every service you rely on, from your bank to your mobile operator, gathers large volumes of information about its users, often from the very start when you initiate the registration. In practice, a broad network of public and private organizations already holds data linked to you.

Social media platforms, search engines, online retailers, tax authorities, hospitals, health insurers and even your employer all play a role in shaping your digital footprint.

Even more unsettling, your data often circulates far beyond the services you knowingly use. It is frequently held by third parties you have never dealt with, companies you may not even know.

This is especially true for **data brokers**: firms whose business model is built entirely around collecting and reselling personal data for advertising purposes. Operating behind largely opaque practices, these companies assemble detailed marketing profiles about individuals and sell them to brands and marketing agencies, often without any clear or informed consent.

Your data is also a valuable commodity for **cybercriminals**. On dark web marketplaces, massive databases containing billions of personal records are bought and sold every day.

These datasets may come from cyberattacks, but they can also be sourced through entirely legal practices such as “data scraping”. “Data scraping” involves the use of automated tools to harvest large volumes of publicly accessible information, from social media platforms, for example.

Why is data so valuable to cybercriminals?

Data is essential to cybercrime. Without information about their targets, cybercriminals simply cannot operate. Personal details, behavioral patterns and digital traces allow cybercriminals to craft increasingly convincing, highly personalized attacks, designed to deceive, manipulate and exploit.

With access to your personal data, cybercriminals can first and foremost craft highly convincing phishing attacks. Phishing involves impersonating banks or official services in order to extract sensitive information.

These attacks typically aim to capture banking details, with the ultimate goal of draining money directly from victims’ accounts. The more personal information a phishing message contains, the more likely it is to be taken seriously.

Quite logically, a message that includes your name, postal address or other personal details is far more likely to inspire trust than a generic communication.

Identity theft is another major risk. By exploiting the data they have collected, cybercriminals can attempt to impersonate you when dealing with third parties such as banks or

telecom operators. They may, for instance, open a line of credit in your name or take out subscriptions without your knowledge. For a resourceful attacker, the possibilities are almost endless.

Data breaches: key figures

According to researchers at Surfshark, a popular VPN provider based in Vilnius (Lithuania), France has recorded an estimated **682.8 million compromised accounts since 2004.**

France is among the countries most affected worldwide. Studies by Surfshark show that France ranked as the most impacted country by data breaches in the third quarter of 2025, ahead of the United States. It means that a

French account is compromised every second. Over the past year alone, around 40 million accounts belonging to French users have been breached.

Which sectors are the most vulnerable?

Given the sensitivity of the data they handle, healthcare organizations are among the sectors most heavily targeted by cybercriminals. By gaining access to medical information, attackers hope to pressure victims into paying a ransom.

As a result, hospitals and medical institutions have gradually become prime targets for data thieves, drawn by the critical and highly sensitive nature of the information they hold.

In France, **749 incidents were reported in 2024** to the CERT Santé, the dedicated incident response team for information systems used by healthcare and medico-social institutions.

Hospitals also frequently suffer from inadequate security measures, often the result of cybersecurity budgets that fall short of the growing threat landscape. The same challenges affect public administrations, which have likewise become one of cybercriminals' preferred targets.

Myths and misconceptions about data breaches

Many internet users still believe that their personal information has little to no value. When we spoke to people around us, several struggled to understand why they should be concerned about the sheer volume of data circulating online about them. Their argument is a familiar one: they claim they have "nothing to hide."

A data breach can have serious consequences, especially for your bank account.

Some people feel reassured simply because they have installed antivirus software on their computer. Yet **an antivirus does not prevent from all attacks, nor does it stop phishing attempts**. It also offers no protection if

your bank or mobile operator is breached and unintentionally exposes your data.

Put simply, antivirus software alone is not enough to guarantee your cybersecurity. The same applies to using a VPN or browsing in Incognito mode. While these tools can be useful, they are far from sufficient on their own to keep you truly protected.

So what can you actually do?

Best practices to protect yourself

Internet users are often advised to secure their online accounts as much as possible, starting with strong passwords. This means choosing a password of at least 12 to 15 characters, combining uppercase and lowercase letters, numbers and special characters. Using a password generator is the safest option.

At the same time, it is strongly recommended to enable two-factor authentication whenever it is available. This security mechanism requires two separate forms of identification to access an account, in addition to a password. Ideally, it should be activated across all your online services.

That said, experience shows that these precautions alone are not enough to fully protect users from data breaches. Once your personal information has been shared with a company, it becomes that organization's responsibility to protect it against attacks.

Whether your account is secured with a strong password or two-factor authentication, your data ultimately depends on the security measures implemented by the entity that holds your information.

There is very little you can do to completely prevent data theft. What you can do, however, is reduce the amount of personal information you share as much as possible.

Start by limiting what you post on social media platforms such

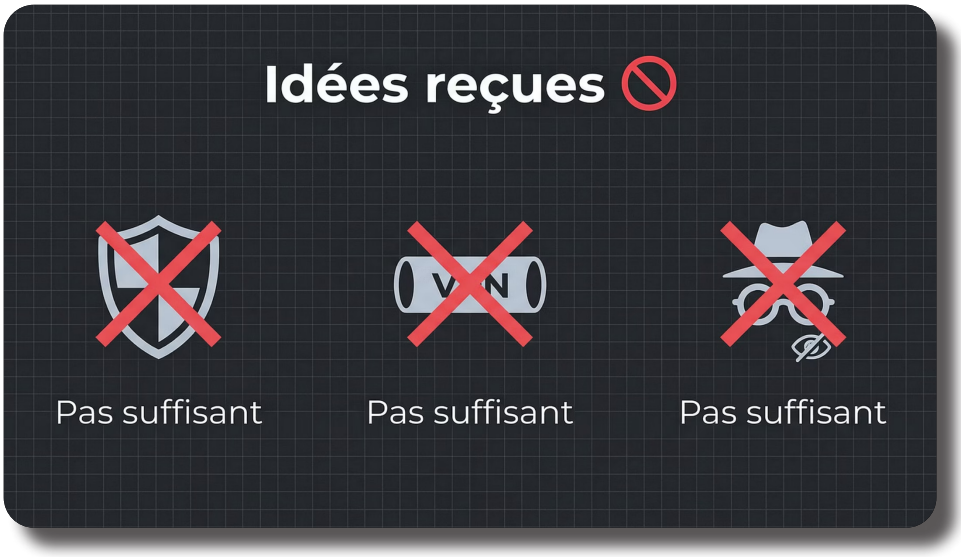
as Facebook or Instagram. On its own, this information may seem harmless, but once combined with data stolen in breaches, it can be used for a wide range of cyberattacks.

Next, try to minimize the number of organizations that hold information about you. If you open an account with an online bank or any other service and no longer use it, think about closing it.

Contact customer support and request the deletion of your personal data under the GDPR (the General Data Protection Regulation). Finally, whenever possible, opt for placeholder or non-essential information. These precautions help reduce your personal attack surface.

Good digital hygiene helps limit how much attackers can learn about you, and how easily they can target you.

Florian Bayard



YOUR SMARTPHONE IS SPYING ON YOU

In France, the average smartphone user installs close to 90 apps on their device. Many of them continuously collect information about our habits, sometimes deeply personal ones. In theory, this data is supposed to remain on our phones. But can we really say that our privacy is fully protected?

To understand how smartphones can monitor their users, we drew on an investigation by the team behind **Cash Investigation** (a French investigative TV programme known for in-depth reports about corporate and economic issues) dedicated to personal data practices.

As part of their report, the journalists conducted a simple but very telling experiment. They purchased a brand-new smartphone, a completely blank device, containing no personal data, and handed it over to computer science expert **Esther Onfroy**, who is a specialist in mobile application analysis.

For the past four years, this engineer has been actively involved in defending digital privacy. She developed a tool that intercepts, in real time, the data smartphones quietly transmit.

From the very moment the phone is switched on, data exchanges begin. Without any action from the user, the device immediately starts communicating, connecting to eleven different servers.

The smartphone tested is a Samsung device, meaning it naturally exchanges data with Samsung services, but also with Google. This comes as little surprise, given that Google owns Android, the operating system powering the phone. Today, Android runs on 86% of smartphones worldwide.

The second stage of the experiment involves downloading an application. Esther then intercepts the data emitted by the phone. Some of this information is sent to Flurry, a firm specializing in marketing and analytics. Much of the data is highly technical and difficult for the general public to interpret.

It includes details such as the phone's activation date, battery level, charging status and even the name of the mobile operator. When is the phone switched on? How long is it used? What actions are performed? All of this information is collected in real time by multiple companies.

Since the experiment began, the device has already communicated more than one hundred times with external servers, including those belonging to Facebook. This happens despite the fact that no Facebook account is installed on the phone. And yet, Facebook is aware that an application is being used.

So how is this possible?

This is largely because most Android apps embed tracking tools developed by Facebook

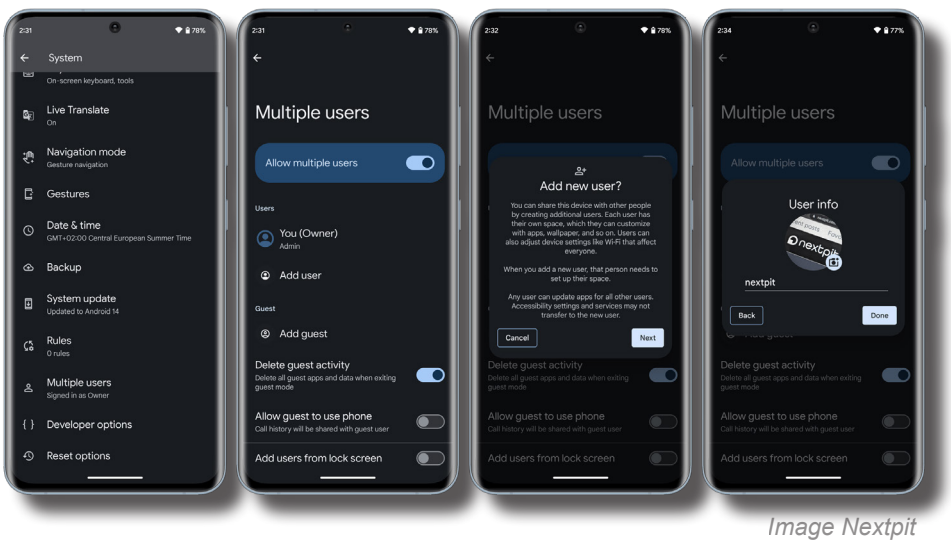


Image Nextpit

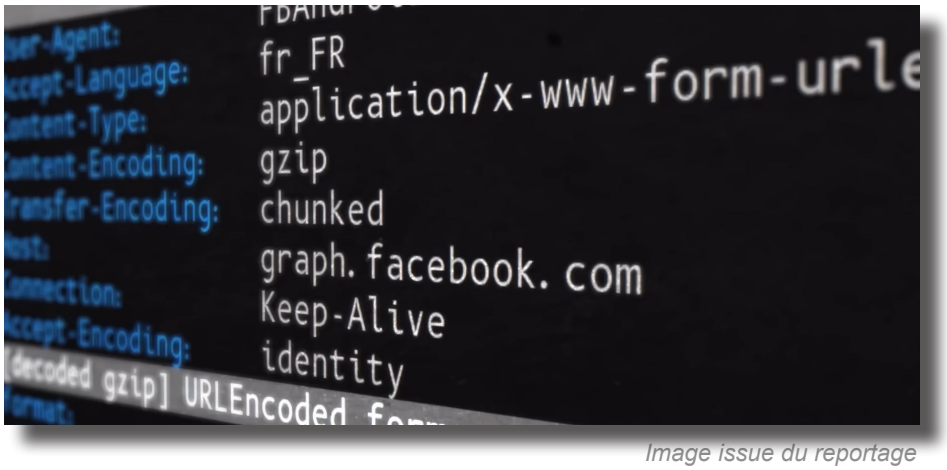


Image issue du reportage

pieces of software designed to collect data on behalf of the US tech giant. Among the information gathered are highly sensitive details, including users' religious beliefs.

Yet the law strictly prohibits the collection or processing of personal data that reveals, directly or indirectly, religious convictions.

So what purpose does this information serve? How is it being used?

This is largely because most Android applications embed tracking tools developed by Facebook. These trackers are designed to collect data on behalf of the US-based company.

Among the information gathered are highly sensitive details, including users' religious beliefs.

Yet the law strictly prohibits the collection or processing of personal data that reveals, directly or indirectly, religious convictions. So what purpose does this information serve? How is it actually used?

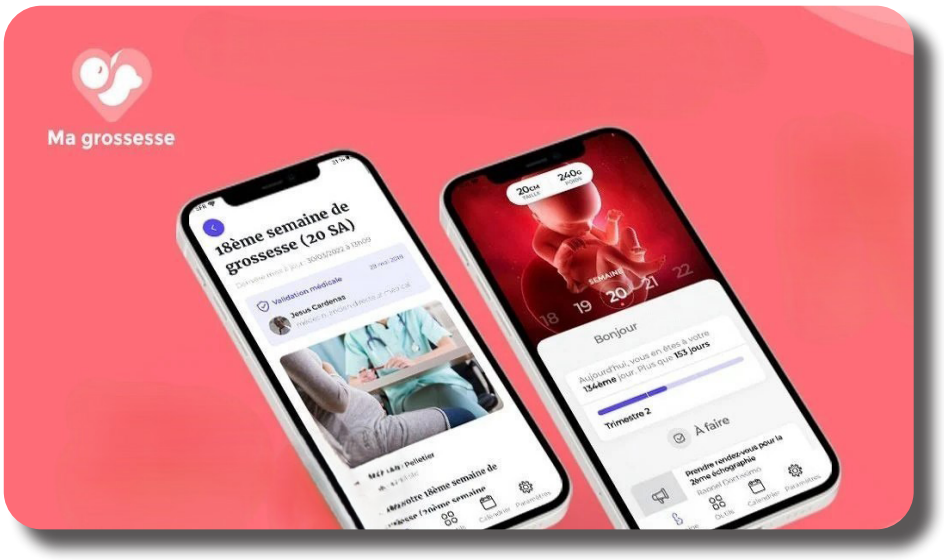
These are not paranoid questions. In November 2020, a major scandal erupted when the prayer app Muslim Pro was accused of sharing the location data of millions of Muslims with the US military. Among them were thousands of users in France, some of whom later filed legal complaints.

And this kind of intrusion can go even further.

Among the most downloaded health apps in France is "Ma Grossesse", an application owned by the Doctissimo group. It allows users to track the development of their pregnancy while entering various personal information, including weight, the hospital where they plan to give birth, the monitoring of contractions and other intimate details.

As part of the investigation, the team entered a weight value and then checked whether this data had been transmitted. They found that information had been sent to the domain profile.localitx.com, operated by Localitx. The data shared included the expected delivery date, the start of the pregnancy and the user's weight.

This means the app transmitted information that makes it possible to infer a user's body mass index (BMI) data that clearly falls under the category of health information. In principle, the transmission of such data is prohibited without the explicit consent



of the individual concerned. Without prior agreement, this information should neither be collected nor leave the device.

Yet in just twenty minutes of use, Doctissimo transmitted around thirty lines of medical data to three commercial partners.

Information relating to contractions and maternity was sent to the French company Xiti. The expected delivery date was transmitted to the US-based firm Localitx, while the 35th week of pregnancy was shared with Google.

The app operates as a powerful tracking tool. There is no denying that the application provides a useful service by helping users monitor their pregnancy. What many users may not realize, however, is that some of the information they enter can be transmitted to and monetized by Doctissimo's commercial partners.

This raises an obvious question: are these data transfers lawful?

To answer it, **Gaëtan Goldberg**, a lawyer specializing in data protection and privacy law, was consulted.

Is Doctissimo entitled to share information that clearly qualifies as health data with third-party companies?

According to him, the principle is straightforward: the processing and sharing of health data with commercial partners is, in principle, prohibited. Any exception requires the company to obtain the user's explicit consent.

What does "explicit consent" actually mean? It requires providing users with clear and understandable information: what data is being collected, who it is shared with, for what purpose, and with what objective.

Users must also be informed whether their data could be used for health-based advertising targeting and they must be free to accept or refuse. In this specific case, however, no explicit consent was ever requested.

Without clearly expressed agreement, the processing of this data is illegal.

Gaëtan Golberg

Image issue du reportage

The team searched everywhere for such a consent notice. When the app is first opened, a pop-up requests permission to process certain types of data, yet it never explicitly mentions health data. They also reviewed the app's privacy policy.

What they found was Doctissimo's data charter: a lengthy document of nearly 5,800 words, which they took the time to read in full. It required thirty-five minutes to get through, a long and painstaking exercise. Even after that effort, much of the content remained difficult to fully understand.

The document is dense, filled with sub-clauses, legal jar-

Image site Doctissimo.fr

gon and technical terminology, creating the impression that it was designed more to confuse than to inform.

For the lawyer, the situation is deeply problematic. Data protection law rests on a fundamental principle: transparency and accessibility. Data processing practices must be explained in a way that is clear, precise and understandable to everyone.

Anyone using the application should be able to determine what happens to their personal data. Instead, what emerges here is a form of systemic opacity, making it extremely difficult for users to understand where their data goes and what risks may be associated with it.

The story takes another turn. When the journalists contact Doctissimo, presenting themselves as users of “Ma Grossesse” and requesting clarification, the company simply replies that no data is shared with partners.

The team then decides to conduct a new experiment directly on the website itself. Psychological tests are one of Doctissimo’s specialties, with nearly 300 free quizzes available.

“What kind of feminist are you?”, “Are you more of a dog person or a cat person?”

Among these questionnaires, one in particular draws their attention: “Feeling down or depressed?”. Thirteen questions later, the verdict is clear: the test concludes that the user shows signs of depression. But a far more troubling discovery soon follows.

Before visiting the site, the journalists installed a free tool called Disconnect, a browser extension designed to identify, in real time, the companies tracking users online. The software reveals which third parties collect data without users’ awareness.

On Doctissimo, the level of activity is striking. Dozens of companies orbit around each visitor, many of them completely unknown to the general public. Were these firms informed that the user had just completed a depression-related test?

In a written response, Doctissimo claimed that it does not collect browsing data that could be considered sensitive, particularly health-related data and maintains that such information is not shared with commercial partners.

Yet just days later, the Cash Investigation team obtained a document suggesting otherwise. The file details the data collected by one of Doctissimo’s partners during their visit to the site.

It lists the exact titles of every page viewed, more than a thousand entries, including the page corresponding to the “Feeling down or depressed?” test.

Why are Doctissimo’s partners tracking users so closely across the web?

It is to refine user profiles and deliver highly targeted advertising. Someone reading several articles about stress may later see ads for calming herbal teas. A visitor browsing sports-related content may be served advertisements for running shoes.

These targeted ads are sold at three to four times the price of standard advertising. They form the backbone of the business model behind free websites such as Doctissimo.

THE HIDDEN SIDE OF OUR DATA: AN INVESTIGATION INTO DATA BROKERS ORGANIZATIONS

Wherever we go, there they are.

Lurking behind our screens, at the pharmacy counter, even within the intimate details of our medical records. An invisible army of companies, known as data brokers, has turned our lives into a lucrative asset.

Masters of the Shadows, a $400 Billion Market

Every click online, every purchase at a pharmacy, every flight search is logged by companies you have likely never heard of.

This investigation highlights a vast personal data market where some of our most intimate details are bought and sold to the highest bidder. Many of these firms operate quietly, shielding their business models from public scrutiny.

Their discretion suggests a clear awareness that their practices may be controversial if not legally questionable.

According to a report by **Knowledge Sourcing**, the global data broker market is experiencing sustained growth.

It is projected **to expand at an annual rate of 7.29% and reach approximately $616.5 billion by 2030, up from nearly $434 billion in 2025.**

The scale of these players is difficult to grasp. The US company Acxiom is said to maintain a database covering 2.5 billion individuals worldwide.

According to **Sarah Spiekermann**, head of the Institute for Information Systems and Society in Vienna, no government anywhere in the world holds a registry of comparable magnitude.

A data broker (courtiers en données) is a company that buys, compile and resells data from multiple sources including websites, mobile apps, loyalty programs, public records and commercial partners in order to build highly detailed profiles of individuals or organizations.

These firms clean, cross-check and enrich the information, they collect age, address, purchasing habits, browsing activity, interests, socio-demographic data, and sometimes financial or health-related elements that are not directly identifiable. The goal is to create targeted segments or scoring models that can be used by advertisers, banks, insurers and other businesses to refine marketing strategies, assess risk, personalize offers or guide commercial decision-making.

Companies such as **Acxiom** and **Experian** are reported to possess what are described as "near-exhaustive" datasets on hundreds of millions of people, with thousands of attributes assigned to each individual.

The Irish data broker Experian claims to hold information on more than 95% of the US population

Source : Experian corporate blog

In Europe, the company is believed to maintain data on nearly 90% of the French population.

Data brokers differ from major digital platforms in one crucial respect: functional invisibility. While users are aware that they interact with companies such as Google, Amazon or Meta, they are generally unaware of the firms operating in the background, collecting, cross-referencing and trading their data.

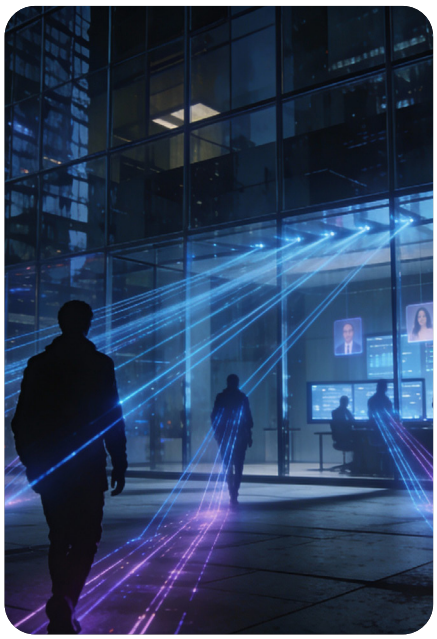
France's data protection authority, the CNIL, describes this as a "complex ecosystem of successive resales," in which a single data point can be copied, enriched and transferred multiple times without the individual ever being informed.

These companies frequently enter into partnerships with one another, exchanging information to further refine and expand individual profiles.

Some of these companies reportedly compile as many as **30,000 distinct data points** per individual. These profiles begin with standard information age or gender but extend far beyond that. They can include frequently visited locations, travel destinations, daily routines, even something as mundane as the coffee someone buys each morning, along with their social connections.

Interests are mapped in detail. So are consumption habits including adult content preferences, income level, social class, political leanings and religious beliefs. And this list represents barely a few dozen criteria, a fraction of the tens of thousands of attributes these firms are said to track.

This level of profiling enables companies to construct a psychological portrait that directly shapes your user experience and what you see online. Most users are unaware that they may be treated differently based on their profile as they browse the web.



The effects become visible, for example, when booking a flight through a comparison platform or directly on an airline's website. Algorithms assess a user's relationship to spending whether they are price-sensitive or willing to pay more. The fare displayed can then adjust accordingly: users perceived as able to spend more may be shown higher prices than others.

The Illusion of Anonymization

To defend their practices, data brokers rely on a now-familiar argument: the data they collect is "anonymized." Without names or surnames attached, they claim it is impossible to identify the individuals concerned.

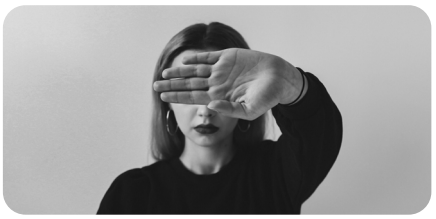
Yet for years, researchers have warned about the serious privacy risks posed by these vast databases.

One of the world's leading experts on data anonymization, **Yves-Alexandre de Montjoye**, a researcher at Imperial College London, has shown that this promise largely amounts to an illusion. Working with an international team, he developed a tool that demonstrates just how easy it is to re-identify someone using supposedly anonymized data.

In one experiment, the researchers worked with an anonymized database containing the profiles of 66 million people in France.

Using only a handful of data points, date of birth, city of residence, gender, marital status and employment status and without even knowing the person's industry, it was possible to accurately identify an individual within minutes, even though the dataset was supposed to be anonymous. These few pieces of information, relatively easy to obtain, are enough to strip away anonymity in a database presented as secure.

Once a profile has been identified, access to the thousands of additional attributes stored in the database becomes possible, revealing a far more detailed portrait of the individual concerned.



Europe to the Rescue?

Since 2018, internet users across Europe have been constantly prompted to give or refuse consent for the collection of their data. In theory, every tracking option can be disabled individually. The process may feel tedious, but it represents a major shift.

For the first time, citizens were given a tangible way to regain control over their personal information.

Unsurprisingly, this evolution was not welcomed by the tech giants.

In an effort to resist the General Data Protection Regulation (GDPR), Google reportedly spent nearly €15.5 million on lobbying activities. Amazon allocated more than €4 million, while Meta and Apple each spent around €3 million.

The pressure campaign led to the submission of nearly 4,000 amendments, making it one of the most extensive lobbying efforts ever witnessed within the European Union. Dozens of lawyers descended on Brussels, meeting with EU institutions, travelling to national capitals and seeking to influence governments and lawmakers in an attempt to slow or reshape the legislation.

If these companies resisted so fiercely, it was because the economic stakes were significant. Recognizing that data belongs to citizens, not platforms, is challenging the very foundation of their business model.

Even when a data access request is properly drafted and clearly asks for a copy of the information a company holds, few organizations comply within the legally required one-month timeframe. Some simply fail to respond. Others claim they hold no data at all while continuing to process or resell it.

Under these circumstances, how much weight can be given to corporate assurances that they do not monetize our data, when it is virtually impossible for individuals to verify such claims on their own?

The GDPR does, however, provide a remedy: any citizen can file a complaint with France's data protection authority, the CNIL. If violations are confirmed, the authority is required to intervene and may impose sanctions on the companies concerned.

In 2025, the total amount of financial penalties exceeded €55 million, including several record-breaking fines. As a result, this trend resulted in an increase in corrective measures compared with previous years. The CNIL has made it clear that it intends to fully exercise its enforcement powers, by relying on a simplified procedure designed to respond swiftly to the most common a data breaches.

IQVIA
THE GIANT TAKING FRANCE' PULSE

A September 2018 ruling by France's data protection authority, the CNIL, authorizes pharmacies to collect several types of data: social security numbers, year of birth, first name, gender, as well as so-called "dispensing data" in other words, a record of all purchased medications. This information can then be transmitted to a US company remaining relatively unknown to the French public: **IQVIA.**

Yet IQVIA is the world's largest broker for medical data.

The company's core business consists of collecting data from hospitals, medical practices and laboratories, and reselling it to pharmaceutical companies. It is a highly lucrative activity: in 2024, the group reported revenue of nearly €15 billion.

The practice has sparked significant controversy across the Atlantic.

Today, IQVIA is one of the largest holders of some of the most sensitive data available, information directly tied to individuals'

physical and mental health. The company gathers everything it can access: prescriptions, medical records and data generated through clinical research, mapping the full patient care journey.

What remains far less clear, however, is how precisely this data is used and how frequently it is resold.

In the United States, the company has faced legal action from pharmacists who accused it of collecting their data without consent. IQVIA was ultimately ordered to pay $10 million in damages. In France, by contrast, the company has secured numerous official authorizations.

For some observers, the situation is deeply concerning. Few people would willingly accept that information as sensitive as their health status or psychological condition could be bought and sold.

This raises a critical question: does the American data broker rely on the same collection methods in France as it does elsewhere?

What is concerning is: **IQVIA has quietly established a presence in nearly half of all of French pharmacies.**

As in any pharmacy, dedicated software records customer information, name, contact details, social security number, attending physician. The system is configured to continuously transmit certain data to IQVIA.

In 2021, roughly half of French pharmacies, around 10,000 in total, were collecting data for IQVIA.

The information transmitted corresponds to pharmacy sales, whether over-the-counter products or prescription medications. In exchange for providing data covering their entire customer base, pharmacists receive a modest monthly payment, along with a tailored market analysis for their store.

Each month, they are sent a summary dashboard detailing sales performance, enabling them to adjust stock levels, refine purchasing decisions and identify emerging consumer trends. They can, for example, track rising demand for homeopathic remedies or dietary supplements in order to anticipate future customer needs.

Data sourced from pharmacies, traded for a few euros and a set of charts, is merged into large-scale databases resold by IQVIA.

As soon as a patient inserts their carte vitale (France's national health insurance card) into the terminal, a unique identifier is generated within IQVIA's system.

This identifier follows each individual across visits to different pharmacies participating in the panel.

Through this mechanism, each transaction can be linked back to a specific person, allowing all medication dispensing records to be consolidated under a single profile.

This form of individualized tracking is highly valuable on the market.

Why such value? Because it is the only database in France capable of delivering market studies of such depth and precision. Some of these studies can reportedly reach €500,000.

And what about the patients ?

Is their consent truly obtained before their data is transmitted to IQVIA?

Under the authorization issued by France's data protection authority, the CNIL, pharmacists are required to inform each customer individually and give them the opportunity to object to the collection of their data.

In practice, however, this obligation is almost impossible to enforce. The reason is simple: time and logistics.

A pharmacist focused on dispensing medication efficiently cannot realistically spend five to ten minutes explaining to every single patient how their data is processed and transmitted. As a result, the information is rarely communicated, and the right to object remains largely theoretical.

Therefore, at Cyber-IT, we decided to contact several pharmacies in northern France to ask a simple question:

were they fully aware of how the data they collected was being processed and shared?

The findings were disturbing. Almost none of the pharmacists we spoke to seemed able to answer the question clearly. One pharmacist, who asked to remain anonymous, admitted he had never realized the data would be treated as a commodity. Had he known, he says, he would never have agreed to take part of this.

Yet within IQVIA, it has long been understood that medical data cannot truly be anonymized.

This observation does not come from an outside critic. It comes from Jean-Marc Aubert himself. Between 2019 and 2023, Aubert served as head of IQVIA's French subsidiary. Since January 2023, he has held the position of Vice President, Healthcare, within the group.

In January 2016, speaking at a business school about the challenges surrounding health data, he explained how individuals can be re-identified within so-called "anonymized" databases.

He also acknowledged the key economic reality that making data genuinely anonymous is not in the financial interest of data brokers.

Anonymizing data generally involves either making it less precise or removing variables that are too identifying

Instead of listing a specific date of birth, for example, a dataset may only indicate an age range. In some cases, certain variables are removed altogether to reduce the risk of re-identification.

But this process comes at a cost: it reduces data quality.

For the company, reduced data quality means reduced commercial value. The more precise the information, the more actionable it becomes and the higher the price it commands.

Interviewed by French journalist Élise Lucet in 2021, Jean-Marc Aubert was questioned about the anonymization of the health data collected by IQVIA.

The journalist confronted him directly: how can the company guarantee to patients that such highly sensitive data, information relating to their physical and mental health, is fully anonymized?

Aubert responded that IQVIA has been working on data anonymization for nearly sixty years. According to him, in six decades of activity, no incidents related to these issues have been recorded. Yet in a notice published on its own website, IQVIA states that the security measures it implements are designed to "reduce the possibility of identification."

The wording is revealing. Reducing the risk of identification implies that the risk does not disappear entirely. It suggests that, at some point, a malicious actor could potentially gain access to a patient's full medical history.

Aubert later clarified that these terms reflect the language used by France's data protection authority, the CNIL. He also acknowledged a significant limitation: certain medical conditions affect only a few thousand people, making anonymization far more fragile.

Since late 2021, IQVIA has introduced a mechanism allowing pharmacists to block the transmission of data from patients who refuse to share their data.

However, during our visits to several pharmacies in northern France, no signage was visible. No information was provided to patients about the collection and transmission of their health data.

A critical question arises: if patients are unaware that their medical data is being collected, are they not deprived of their rights? In particular, the right to object, one of the core principles of the GDPR.

How can someone exercise a right if they do not even know they are concerned?

We reached out to France's data protection authority, the CNIL, to address these specific questions. Despite a first encouraging discussion and several follow-up requests, the authority ultimately declined to comment.

For several years now, the American company IQVIA, specializing in health data analytics, has been seeking access to increasingly detailed medical information, including hospital records. The company has shown particular interest in cancer-related data, a field that sits at the heart of the pharmaceutical industry due to the significant medical and financial stakes involved. This raises broader questions about how health data is handled in France.

A shift in scale is now taking shape with the rollout of a national framework to centralize health data. Publicly announced by the French President of the Republic in March 2018, this ambitious initiative aims to establish a true “health data hub” designed to gather and structure all data generated by the French healthcare system.

The objective is to centralize reimbursement data from the national health insurance system, hospital clinical information, data from private practitioners, as well as large scientific data and registries, making them more readily accessible for research and also providing an overall improved care system experience.

Known as the Health Data Hub, this framework compiles data from hospitals, clinics, elderly care facilities, medical laboratories, pharmacies, private medical practices, and radiology centers.

It brings together nearly twelve years of data covering the entire French population

According to France’s data protection authority, the CNIL, the platform is designed as a secure technological environment intended to store, process and analyze data under strictly regulated conditions. Yet the legal framework governing the Health Data Hub has also relaxed the conditions for accessing medical data. It is no longer necessary to justify a specific research project, study or evaluation in order to obtain access.

Invoking the notion of “public interest” now suffices, a deliberately loosely defined concept. This ambiguity raises many questions. What exactly falls under the scope of public interest, and how far can it reasonably extend? For example, could an insurance company request access to the Health Data Hub on the grounds that reducing costs for a given population serves the public interest? The concept lacks clear boundaries.

Yet, another factor also complicates this project. The government entrusted the rollout of the Health Data Hub to Jean-Marc Aubert, then a senior executive at IQVIA. He stepped away from his role within the company for two years to lead the project.

The fact that the Health Data Hub was designed and implemented by someone coming from the data brokerage sector has drawn sharp criticism.

Concerns intensified when, just one week after the platform’s launch, Jean-Marc Aubert returned to IQVIA France as its president. The debate over potential tensions between public responsibilities and private interests quickly moved to the forefront.

Jean-Marc Aubert stated that, during his assignment for the French state, he filed the required declarations with the High Authority for Transparency in Public Life and appeared before the ethics commission responsible for reviewing potential conflicts of interest. His return to IQVIA was also formally declared and reviewed by the same authority.

IQVIA France maintains that there is “no conflict of interest” in Jean-Marc Aubert’s professional career path.

As concerns grew around privacy issues, governance and the potential commercial use of health data, several former public officials and political leaders chose to speak out publicly.

Among them was Adrien Parrot, who supervised database management at Assistance Publique - Hôpitaux de Paris when the Health Data Hub was launched in 2019. Philippe Latombe, Member of Parliament and Secretary of the National Assembly's Standing Committee on Constitutional Laws, also raised questions about the initiative.

INTERVIEW ADRIEN PARROT

Adrien, thank you for accepting our invitation to share your perspective. We would like to take you back to 2019, when the Health Data Hub was being set up, and hear your insights on the context at the time.

At the time, I was working as an engineer within AP-HP's (Greater Paris area hospitals organization) health data warehouse, the public hospital network of Paris, which in many ways serves as a counterpart to the Health Data Hub. Given my position, I was bound by a fairly strict duty of discretion. As an engineer, I was closely involved at the early stages of the initiative.

The technologies selected by the engineering teams, including Nicolas Paris who had joined before me, as well as several others, were based entirely on open-source software. The infrastructure was fully self-hosted, reflecting a deliberate choice in favor of technological independence and control. The entire system was hosted on AP-HP's own servers.

At the time, we had managed to deliver, broadly speaking, the same core functionalities that were being envisioned for the Health Data Hub during its initial planning phase.

Then, in May and June 2019, internal emails revealed that the Health Data Hub project, which we did not oppose in principle, would ultimately be hosted on Microsoft Azure. From that point on, internal resistance began to grow steadily.

In late 2019, we published a piece in Le Monde newspaper, followed by legal challenges before the Conseil d'État. Shortly thereafter, Nicolas Paris and I decided to leave AP-HP. At the time we wrote that piece, the AP-HP data warehouse was already fully operational. We were not speculating or engaging in abstract debate. We knew there was a viable alternative because it already existed. AP-HP had built it. It was based on open-source technologies that were well understood, fully controlled and technically mature.

Back then, questions of digital sovereignty were far less significant in the public debate. It was only after conducting a detailed legal risk assessment with lawyers that we came to an alarming conclusion: choosing American cloud technologies was a problem. In our view, it jeopardized medical confidentiality.

The concern was that the data were easily accessible to non-European entities, without adequate protections aligned with European Union standards. What followed

was not just a technical disagreement, but a broader conflict of principles rooted in ideological, technical, ethical and professional considerations. At that point, we felt we had no choice but to take a stand.

I'm not sure how much you're able to comment on this, but there has been considerable discussion around Jean-Marc Aubert and IQVIA, particularly regarding the role he was given in setting up the Health Data Hub. What do you think about this situation?

I'll stick to the facts. Others, including Le Monde, have raised concerns about potential conflicts of interest and the so-called "revolving door" dynamic in Jean-Marc Aubert's case.

As for the decision to select Microsoft, I have no information suggesting that any payments were made, and I cannot speculate on that.

What can be said, however, is that when you are familiar with certain technologies, especially those used by a company like IQVIA, there is a natural tendency to favor what you already know. Not necessarily because of any form of compensation, but simply out of professional reflex. When you understand a tool, you are more inclined to rely on it to meet a given need. That, in itself, is fairly typical.

That said, IQVIA does not rely on European open-source technologies to process this kind of data. At the time, the company was familiar with using specific cloud infrastructures, and it is likely that those same environments remain in use.

So there was, at the very least, this dynamic: a tendency to promote solutions they were already familiar with, even if those solutions were not necessarily aligned with the public interest or with the broader interests of French citizens and the French state.

In your view, what is the real risk of having our data placed in the hands of non-European actors?

The issue at stake is fundamental freedoms and medical confidentiality.

This is precisely what Edward Snowden exposed when he revealed the scope of mass surveillance programs such as PRISM, as well as the broader implications of legislation like the U.S. Cloud Act. National security laws in the United States can be far more permissive, allowing wide-ranging access to data under certain conditions.

These legal frameworks were at the heart of the challenges brought by Max Schrems, which ultimately led to the invalidation of successive transatlantic data transfer agreements designed to authorize data flows between Europe and the United States.

One of the central risks, therefore, is the possibility of data being accessed outside a framework that meets European legal standards.

For European citizens, when their data is hosted by non-European cloud providers, they may find themselves in a legal grey zone. If they seek legal action or simply wish to exercise their rights, the process becomes significantly more complex, if not practically impossible.

From our perspective, that is not an acceptable situation.

We should not remain in a legal environment that does not effectively allow individuals to exercise their GDPR rights, whether that is the right to object, to rectify inaccurate data, or to request its suppression.

For us, the primary issue remains one of fundamental freedoms and medical confidentiality.

But the risks extend well beyond that.

There is, first, the risk of service disruption. One striking example involved a judge at the International Criminal Court whose access to cloud services and Microsoft Teams was abruptly suspended under the Trump administration. When critical services can be switched off overnight, the implications are significant.

Another growing concern, particularly for chief information officers, relates to cost escalation and licensing models. For essential public services, national research infrastructure, or any mission-critical system, once an organization is locked into a specific cloud provider, it may have little choice but to absorb successive price increases.

Over time, this can become financially unsustainable. Hospitals are already experiencing this pressure, whether with virtualization technologies or even basic email services. The economic stress is real.

In short, the tangible risks include threats to fundamental freedoms, potential service interruptions, restricted access, and financial dependency.

We have taken these concerns before the Conseil d'État twice with the association Interop, in fact three times across two separate issues: the Health Data Hub itself, and later during the COVID-19 vaccination campaign. The legal arguments were similar, as some appointment-booking platforms relied on American cloud providers. Doctolib, for instance, is hosted on Amazon's infrastructure.

And that is only part of the story. There is so much more to say…

INTERVIEW PHILIPPE LATOMBE

At the time, we expressed serious concern in our report about the decision to host the entirety of the Health Data Hub's data with Microsoft, specifically on its Azure cloud platform, and to do so without a formal public tender.

We were told that, during the initial build phase, relying on the "Union des groupements d'achats publics" (UGAP), France's central public procurement institution, was sufficient and made a separate public bidding process unnecessary.

Members of Parliament later questioned the relevant ministers during official government Q&A sessions. Both the Minister of Health and the Secretary of State for Digital Affairs gave the same response in the Senate and the National Assembly: the hosting arrangement was said to be reversible, with a planned transition from Microsoft to a sovereign provider, in line at the time with the "cloud at the center" doctrine, later reframed as the "trusted cloud" strategy.

This migration was expected to take place within eighteen months. Yet three years later, it has still not been implemented.

For months, I have submitted questions to the

Health Data Hub without receiving relevant answers.

I have requested specific documents, including copies of contracts, the number of consultants involved, their daily or hourly rates, and details of the work they carried out for the Health Data Hub. The goal was to better understand the strategic decisions that led the project not to follow through on the commitments publicly announced by ministers.

In response, the Director of the Health Data Hub simply advised me to file a request with the Commission for Access to Administrative Documents (CADA).

The Health Data Hub has argued that no viable French alternative existed. It suggested that launching a public tender could even have harmed the domestic industrial landscape, on the grounds that no French or European company would have been selected, thereby highlighting the competitive gap with American providers.

Are there solutions available to host this data? Yes.

Several French companies are fully capable of doing so, including OVH, Scaleway, NumSpot, Outscale and Cloud Temple. There is a large range of option. Universities and research laboratories already rely on the Secure Data Access Center (CASD), a solution that was referenced in a report on health data by Marchand-Arvier, a member of the Conseil d'État and now chief of staff to Minister Vautrin.

I am not prepared to dismiss the possibility that the Health Data Hub faces a form of dependency on Microsoft and its Azure cloud. That question deserves a thorough and transparent examination. I do not subscribe to conspiracy theories, but the complete absence of reversibility for more than five years, despite repeated ministerial statements, is a concern.

" The law will need to evolve to make immunity from non-European extraterritorial legislation the standard for sensitive data, particularly health data belonging to French and European citizens

On July 1, 2025, acknowledging the tension between the extraterritorial reach of U.S. legislation and the need for greater digital sovereignty, the Health Data Hub launched a public tender. The contract, estimated at €6.2 million over four years, remained open until August 4, 2025, with deployment scheduled for summer 2026. OVHcloud and Cloud Temple have confirmed that they submitted bids.

Credit photo : Philippe Latombe - JOEL SAGET / AFP

DARKWEB
The New Digital Wild West

INSIDE THE LUCRATIVE TRADE OF PERSONNAL DATA

SPECIAL REPORT

A billion-dollar underground economy thriving beyond any legal control.

While major technology companies build their empires on personal data, a parallel market is flourishing in the shadows of the web.

On the dark web, a network of decentralized platforms hidden behind multiple layers of encryption, stolen personal information is traded like financial assets. The volume of this underground business is significant.

The numbers speak for themselves. As of 2025, more than three million people access dark web platforms every day, and an estimated 60 percent of active domains are linked to illicit activity.

This shadow economy generates roughly $1.5 billion annually

Through the sale of stolen data, counterfeit goods and other illegal products. Within that ecosystem, personal data occupies a central role.

An estimated 15 billion compromised accounts are currently circulating on the dark web, representing an 82 percent increase since 2022. This surge reflects a simple dynamic: the harder data is to obtain, the more valuable it becomes.

What exactly is the dark web ?

The dark web is a specialized segment of the internet that requires dedicated software to access and is deliberately hidden from traditional search engines.

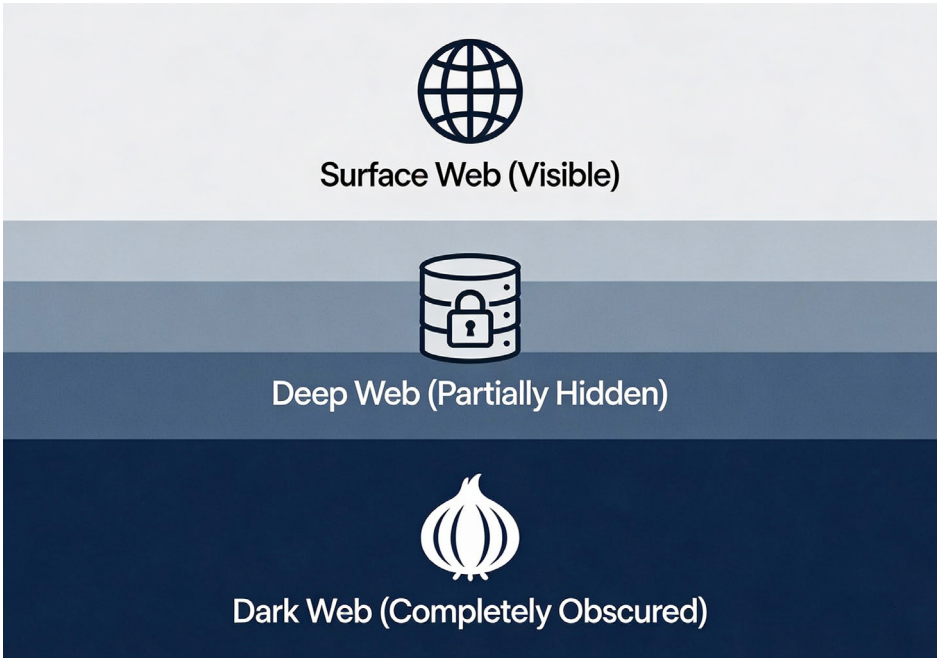
It is important not to confuse it with the “deep web,” a common but misleading misunderstanding.

The deep web simply refers to content that is not indexed by search engines, representing roughly 96% of the internet. This includes your email inbox, online banking statements, digital medical records and subscription-based scientific databases. In other words, most of what we use daily online sits within the deep web.

The origins of the dark web goes back to the 1990s. The Tor project was initially developed in 1995 by the U.S. Naval Research Laboratory to secure government communications. Its principle was straightforward: route data through multiple encrypted relays to obscure both its origin and destination, making user tracking extremely difficult.

What began as a government security tool gradually became available to the public.

In 2003, Tor’s source code was released as open source, allowing developers worldwide to build applications and services on top of it. What could have remained primarily a privacy tool for journalists and dissidents operating under repressive regimes has, over time, also become a preferred environment for criminal activity.



How Tor and the Dark Web Work ?

To understand why the dark web is so difficult to regulate or monitor, we should look at how the Tor network operates from a technical standpoint.

Under normal circumstances, when you send data over the internet, it travels directly from your device to the destination server. Along the way, traces are left behind: your IP address is logged, and some servers can see where the traffic comes from and where it is headed. This visibility is what allows governments and internet service providers to monitor online activity.

Instead of sending data straight to its destination, Tor wraps it in multiple layers of encryption, which explains the name "onion routing." The encrypted traffic is then routed randomly through a series of servers, known as relay nodes, distributed across the globe.

Here is how the process works:

1. Your computer encrypts the data and sends it to a first relay node.

2. That node decrypts one layer, revealing only the address of the next node, not the final destination.

3. The next relay removes another layer, without knowing either the original source or the ultimate destination.

4. This process repeats across several relays, typically three to five.

5. The final relay, known as the exit node, sends the decrypted traffic to the destination server.

The result?

No single relay has full visibility over both the origin and the destination of the data.

Even the destination server cannot determine the true source of the traffic. Only the exit node sees the decrypted content, and it does not know the identity of the original user. This architecture is what makes the network resilient, but also extremely difficult to control.

DARK WEB MARKETPLACES

Once connected to the dark web via Tor, users can access underground marketplaces hosted on .onion domains.

These platforms operate much like traditional e-commerce websites. They feature vendors and buyers, customer reviews, private messaging systems, and escrow mechanisms designed to secure transactions.

The difference is in what is being sold.

Products range from narcotics and firearms to forged documents, hacking services, and, of course, stolen personal data.

The ecosystem is typically hierarchical. Smaller niche markets coexist alongside large generalist platforms. Blacksprut, for instance, currently holds an estimated 28 percent market share, making it one of the largest active dark web marketplaces.

Yet the landscape remains highly volatile. Most platforms frequently disappear, either due to law enforcement action, internal disputes, or so-called "exit scams" where operators vanish with users' funds.

On March 21, 2023, BreachForums was shut down following the arrest of its administrator, Conor Brian Fitzpatrick.

The forum later resurfaced under the leadership of the hacking group ShinyHunters and a former BreachForums administrator known as "Baphomet."

It was seized again on May 15, 2024, before reappearing within hours after the domain was reclaimed.

HOW DOES A DARK WEB MARKETPLACE WORK ?

Registration and Authentication

To access a restricted marketplace, users need to create an account with a username and password. Some platforms require invitations or endorsements from existing members, adding an additional level of gatekeeping to the matter.

Browsing and Searching

Once registered, users can explore product categories or use search tools to locate specific types of data.

Vendor Listings

Sellers publish listings describing the data or services they offer. A typical example might read:

"Verified medical records, U.S. patients, 2020-2024. 10,000 records for $25,000. Instant delivery."

Payment

Transactions are generally conducted in cryptocurrency, most often Bitcoin. Payments are commonly held via Escrow services: the platform temporarily retains the funds and releases them to the seller only once the buyer confirms receipt of the product.

Delivery

Data is delivered through encrypted download links or as files shared via private messaging systems.

Reviews

After a transaction, buyers can rate the seller and leave feedback on data quality and reliability. It is what builds long-term reputation.

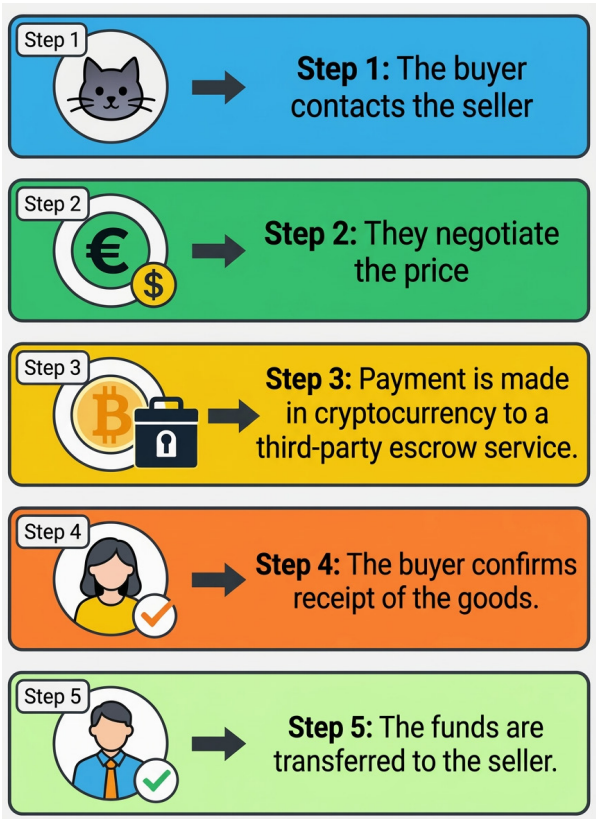
The Dark Web Community

Beyond the marketplace transactions, the dark web functions as a loosely connected but highly active community. There are beginner guides, technical discussions, and even legal advice.

The user base is diverse. It can include professional cybercriminals, data thieves, scammers, and drug traffickers. But there are also political activists, dissidents operating under authoritarian regimes, investigative journalists, whistleblowers, and privacy-conscious individuals.

This mix is precisely what makes the dark web so complex to regulate. A ban would harm activists and vulnerable individuals who rely on anonymity for protection. Yet, it entirely unchecked risks allowing organized crime to operate freely.

This tension is central to the debate.



THE DIFFERENT TYPES OF STOLEN DATA & WHAT THEY ARE WORTH

On the dark web's black market, not all data is created equal. Its value depends on several factors: how complete the information is, how recent it is, and how useful it is for criminal purposes.

Vendors typically organize their offerings into structured catalogs.

At the top of the hierarchy are so-called "fullz" packages.

A fullz bundle contains everything a criminal need to fully impersonate someone, both online and offline. These packages usually include a name, date of birth, address, Social Security number or national ID number, and often financial information.

Pricing varies depending on the quality of the data and the victim's country of residence. According to cybersecurity researchers' findings in 2025:

Basic fullz (developing countries): $6-$12

Standard fullz (developed countries): $20-$100

Premium fullz (with strong credit profile): $150-$250

It's disturbing: an entire identity, built over years through credit history, financial records and reputation, can be sold for the price of a pizza.

Government-issued identifiers are in high demand. U.S. Social Security numbers, European national insurance numbers and similar IDs are traded widely:

Standalone Social Security number: $1-$6

Validated Social Security number: $8-$15

Passport or driver's license: $500-$3,000

A single Social Security number is relatively easy to fabricate or exploit, given its predictable structure. But a valid passport or driver's license is way harder to replicate and can enable higher-level fraud, such as opening bank accounts or securing loans.

Banking and Financial Information

Stolen financial data sits at the core of the dark web economy. It provides direct access to a victim's assets. A compromised bank account is not only a privacy breach, it is a clear financial theft. Prices vary depending on the level of access:

Online banking credentials: $200-$1,000

Credit card number (basic): $5-$25

Credit card with CVV security code: $25-$120

Full credit card dumps (number, CVV, cardholder details): up to $500 for high-end credit cards

U.S. credit cards generally command higher prices. This reflects stronger purchasing power and typically higher credit limits.

Beyond raw financial data, sellers also offer direct access to online accounts, often referred to as "compromised accounts" or "logins."

Social Media and Digital Accounts

Netflix : ~5$
Spotify : ~3$
Premium Instagram account: ~ $20
Email accounts (Gmail, Yahoo, Outlook): $10-$50 depending on account activity history

Cryptocurrency and Digital Wallets

Accounts containing crypto assets or funds in e-wallets can sell for $1,100 to $2,000, particularly when they hold significant balances.

Administrator Access to Corporate Systems

$500 to $100,000, depending on the size and strategic value of the company.

When a hacker obtains the credentials of an IT administrator within a large organization, the value of that access can be enormous. It can be used to deploy ransomware, exfiltrate sensitive corporate data, disrupt operations, or resell the access to other criminal groups.

Medical Records

Among all categories of stolen data circulating on the dark web, comprehensive medical records are among the most expensive.

At first, this may seem surprising. Why would a medical file be worth more than direct access to a bank account? The answer lies in the versatility of medical data for criminal exploitation.

A complete medical record can allow criminals to submit false health insurance claims, purchase prescription drugs under a victim's identity, create a fraudulent medical identity, exhaust a victim's insurance coverage, leverage medical history in loan or insurance applications.

According to 2025 data, medical records are priced as follows:

Basic medical file: $50-$150

Comprehensive medical file with full insurance history details: up to $500 or more

Highly detailed medical records: $250-$1,000

Location Data and Metadata

Modern technology generates vast quantities of metadata. Location data, in particular, has become a valuable asset.

Every time you use an app, make a phone call, or browse the web, your location may be recorded. Over time, this creates a detailed map of daily routines, habits and movements.

An investigation conducted by Datarade in 2025 revealed that location data from millions of individuals had been sold, in some cases through channels that were technically legal, with data brokers transferring datasets to unknown buyers.

Pricing typically follows this structure:

Raw location data (per data point): a few cents per record

Aggregated location datasets (millions of points): $10,000 to $1,000,000 depending on granularity and geographic scope.

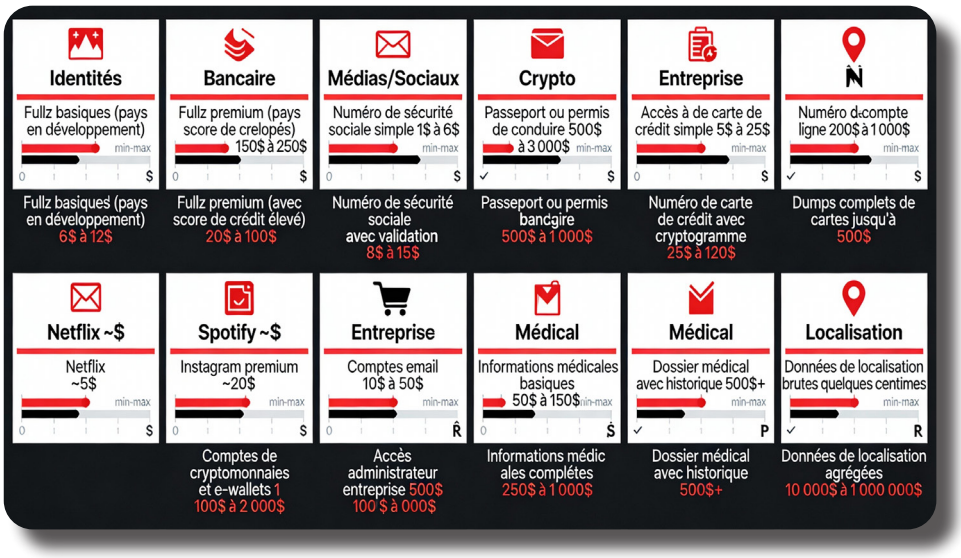
Data Involving Children and Minors

A particularly disturbing segment of the dark web economy involves data related to children and minors. This type of data is highly valued for purposes including exploitation, trafficking and financial fraud targeting minors.

Out of respect and responsibility, specific pricing details are not provided here.

What must be noted, however, is that crimes involving minors remain among the most serious offenses and are proactively pursued by law enforcement agencies worldwide.

Source : deepstrike.io



HOW IS PERSONAL DATA STOLEN ?

Before data appears on the dark web, it must first be stolen.

Understanding how this theft occurs is essential to grasp why this practice has expanded so rapidly.

Stolen data originates from multiple sources, each representing a distinct attack method.

Large-Scale Data Breaches

The most visible source of stolen data remains large-scale breaches.

When a hacker infiltrates the servers of a major corporation or government agency and extracts vast quantities of personal information, millions of records can suddenly flood underground markets.

Data breaches typically occur through several recurring methods:

Exploitation of Software Vulnerabilities

An attacker identifies a flaw in a web application's code that allows unauthorized access to the database. Some vulnerabilities can remain undetected for years before being discovered and exploited.

Phishing and Social Engineering

Attackers send emails that appear to come from trusted sources, such as banks or social media platforms, encouraging employees to enter their login credentials. Despite their simplicity, these tactics remain highly effective. A single employee clicking on a malicious link can grant attackers access to an entire corporate system.

Compromise of Administrator Accounts

Administrator accounts carry elevated privileges within an organization's infrastructure.

If attackers can obtain or guess administrative credentials, they can potentially access all data stored within the system.

This can occur through weak passwords, poorly configured account recovery mechanisms, credential theft, or manipulation techniques that trick administrators into granting access.

Malware and Ransomware

Malware refers to malicious software designed to infiltrate a victim's device or an organization's systems. Once installed, it can log keystrokes, exfiltrate files, or create backdoors for persistent access.

In ransomware attacks, data is typically copied before being encrypted. Even if the victim pays the ransom, stolen information may still be sold on the dark web.

Cloud Backup Exposure

Many organizations store backups in cloud environments. If these backups are not properly encrypted or securely configured, attackers may gain direct access to them. Misconfigured storage buckets and weak access controls remain common points of failure.

Data Sourced from Data Brokers

There is also a legal or semi-legal dimension to the data economy, explored earlier.

Some datasets later found on the dark web originally come from legitimate data brokers. In some cases, these brokers are themselves breached. In others, datasets are resold, aggregated or leaked in ways that blur the line between legal trade and illicit circulation.

Publicly Accessible Data

Not all personal data sold on the dark web is obtained through hacking.

A significant portion is compiled from publicly available sources. Names, addresses, phone numbers and professions can often be found through online directories, property registries, digital business listings and social media platforms.

Attackers can use automated scripts to scrape these sources and consolidate the information into structured databases, which are then packaged and sold.

Corrupt Employees

Sometimes, data is not stolen by external attackers but by insiders.

Resentful or financially motivated employees with legitimate access to sensitive systems may copy and sell data. Insider threats are particularly dangerous because these individuals often bypass external security measures. They know where critical information is stored, how monitoring systems operate, and how to avoid detection.

The Money Flow

How does money circulate within the dark web economy?

The process is layered and designed to hide its origins.

Negotiation and Sale
Prospective buyers contact vendors directly, negotiate pricing, especially for bulk datasets, and complete transactions using cryptocurrency.

Money Laundering
Cryptocurrency received from dark web transactions must eventually be converted into usable funds. This typically involves several steps.

a. Peer-to-Peer Exchanges

Cryptocurrency may be traded directly with other users in exchange for different digital assets or for traditional currencies.

b. Mixing Services

To make tracing more difficult, funds are routed through "mixers". These services mix and redistribute cryptocurrency from multiple users, breaking the transactional link between sender and recipient and complicating forensic tracking.

c. Conversion into traditional currencies

Eventually, the cryptocurrency is converted into traditional currency through exchanges or intermediaries. This often occurs through multiple smaller transactions to avoid triggering reporting thresholds or compliance checks.

Final Use
Once laundered, the funds can be used to purchase goods, finance further criminal activity, or be reinvested into other ventures within the underground economy.

THE IMPACT ON THE VICTIMS

The exposure of personal data threatens a fundamental right: privacy. But the impact does not stop there.

Financial Loss

The most immediate consequence is often financial. A criminal with access to your bank account can simply drain it. With stolen credit card details, fraudulent purchases can be made until the credit limit is reached.

According to the FBI, reported online fraud losses in the United States totaled $12.5 billion in 2023, based on 880,418 complaints, representing a 22 percent increase compared to 2022.

Identity Fraud: accounts opened in the victim's name

A more insidious risk arises when criminals open new bank accounts, apply for credit cards, or take out loans using a victim's identity. In many cases, the fraud goes unnoticed for months. The first sign of trouble comes in the form of a letter demanding payment for an account the victim never opened.

Tax Fraud

An identity thief can use your tax information to file a fraudulent tax return and claim a refund in your name. In many cases, victims only discover the fraud when their legitimate filing is rejected or flagged by tax authorities.

Credit Abuse

Criminals may also take out loans in a victim's name and fail to repay them. Meanwhile, the victim's credit score deteriorates. This can significantly impact their ability to secure financing for major purchases, such as a car or a home.

Medical Fraud

If a victim's medical records are stolen, a criminal can exploit their insurance coverage to obtain expensive treatments.

The fraud often comes to light only later, when the victim receives a bill for services they never used, or discovers that their insurance coverage has been completely consumed by fraudulent claims.

Loss of Insurance Coverage

If you have health insurance and a criminal exploits your coverage for expensive treatments, your insurance company may terminate your insurance policy. Even though you are the victim, you may still lose your insurance.

Fraudulent Prescriptions

Criminals may also use your identity to obtain prescription drugs, including opioids and other controlled substances. Beyond the financial damage, it can leave a record suggesting you obtained controlled substances you never requested, which could lead to serious legal complications.

Professional and Legal Consequences

Victims of identity fraud are often left to start the recovery process by themselves.

They must prove that they are not responsible for the fraudulent activity, victims must prove they were not responsible, instead of the focus being placed on the criminal or the institution's failure to prevent the fraud.

Fraudulent Criminal Records

In the most extreme cases, a criminal may commit offenses using a victim's identity. As a result, your name can be linked to crimes you never committed, creating a digital criminal record that does not belong to you.

Employment Impact

Employers routinely conduct background checks on job applicants. A record tainted by identity fraud can disqualify someone from various roles, particularly positions that require trust or access to sensitive information.

A Lasting Criminal Record

Even after proving that you were not responsible for the offenses committed in your name, traces of the record may remain in public databases. Future employers or business partners may still see that a criminal entry exists with your name, regardless of the circumstances.

Psychological and Emotional Impact

How long does it take to fully recover from identity theft ?

Unfortunately, there is no simple answer to this question. It depends on the scope of the fraud. In easier cases, such as a single fraudulent account, the issue may be resolved within a few weeks. In more complex situations, however, the process can take months, or even years.

Psychological Trauma

Victims can struggle with anxiety and emotional distress. Discovering that someone has taken over your identity, pretending to be you, and dealing with financial institutions or government agencies in your name can be very disturbing.

Chronic Stress

Recovering from identity fraud is rarely quick. The process can take months, sometimes years. During that time, victims often live in a state of uncertainty, anticipating the next discovery, the next call from a financial institution, or the next letter from the bank.

Social Isolation

Feelings of shame can push some victims into isolation. They may internalize the incident, even though responsibility lies entirely with the criminal.

Identity fraud is not only a financial crime, it is also an emotional burden that can linger long after the technical breach has been resolved.

INSIDE THE NATIONAL CYBER UNIT

Hervé Petry

Commandant,
National Cyber Unit

Could you introduce the National Cyber Unit?

The National Cyber Unit (UNCyber) operates within the National Judicial Police Unit (UNPJ), which serves as the operational section of the French Gendarmerie in cyberspace. As a national criminal investigation unit headquartered in Pontoise, just outside Paris, UNCyber leads high-level investigations into major cybercrime cases across the country. The unit coordinates the work of the 26 UNCyber regional units and the ten thousand gendarmes

Three missions:

- **Cyber Intelligence**
- **Investigations**
- **Technical support**

who make up the Cybergend framework, extending its operations across France as well as French overseas territories.

UNCyber is structured around three divisions counting 120 people.

The Intelligence and Coordination Division (DARC) provides specialized support functions, including field intelligence, technical intelligence, the CERT-GN cyber response team, and both national and international coordination.

The Operations Division (DO) leads investigations into organized cybercrime at both national and international levels, covering areas such as child exploitation, ransomware, online fraud, and online trafficking.

The Technical Division (DT) delivers technical and digital forensic support. It deploys specialist qualifications to assist local units and leverages advanced data analysis tools to support investigations.

Since February 1, 2024, UNCyber has been commanded **by General Hervé Petry.**

What is UNCyber's role in combating data theft?

UNCyber plays a central role in investigating and coordinating responses to large-scale data theft cases. The Operations Division is responsible for leading complex cybercrime investigations, including cases involving data breaches, ransomware operations, and organized data trafficking networks. In addition, the unit includes a specialized branch within its organized crime department, known as the STAD group (focused on attacks against automated data processing systems).

This unit was created to provide an operational response to a growing reality: small and medium-sized businesses but also local authorities, are increasingly being targeted by ransomware attacks. Large corporations are not spared either. These incidents frequently involve data exfiltration and ransom demands, leading to severe disruption of IT infrastructure when systems are under malicious control.

The economic consequences can be significant and extortion remains the main motive. Attackers demand payment in exchange for restoring access to encrypted systems or for promising not to expose the stolen data. These attacks also have a direct impact on citizens, particularly when essential services or public institutions are affected.

The STAD group's cyber investigators specialize in data theft cases, a modern form of cybercrime that is often linked to organized criminal networks.

In today's geopolitical climate, cybercrime has become a critical and deeply serious issue.

Cybercrime is constantly evolving. It is a threat that adapts and reaches into every layer of society. Cyberattacks cause considerable damage, affecting individuals and businesses, causing serious damage.

Do you have recent data to illustrate the ongoing situation ?

2024 data confirm the trend:

348,000 RECORDED CYBER OFFENSES

representing a 74 % increase over 5 years

- **65 % involved financial harm**
- **29.7 % targeting individuals**
- **4.9 % affecting institutions**
- **17,100 attacks against information systems**

What kind of data are criminals actually looking for, and why?

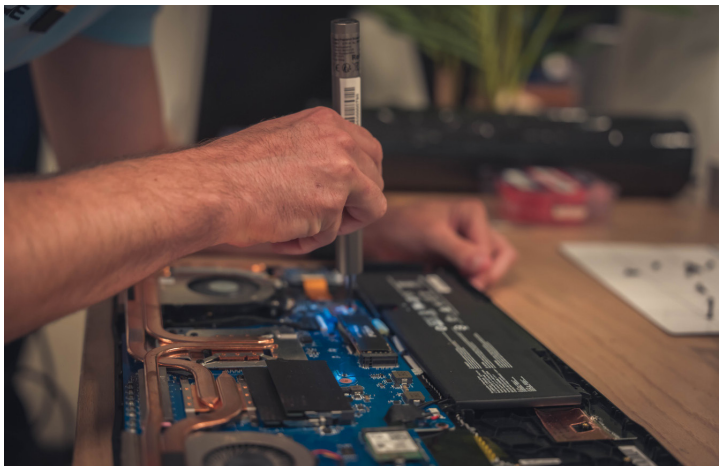
In reality, almost any piece of personal information can have value. Basic identity details such as a date of birth, home address, email, phone number, social security number, or banking information can all be turned into money. That data may be resold, used to run scams, impersonate someone, apply for loans, or claim public benefits under false identities. The uses are varied, but the objective is always the same: financial gain.
.

What does a typical day look like for investigators working on the clear web and the dark web?

There is no real typical day. Every case brings its own challenges.

The investigators work involves monitoring online activity, shadow forums, and hacker communities, as well as keeping an eye on marketplaces where stolen data may surface. It also means analyzing platforms that could

Credit : Unité Nationale Cyber



be used to exchange or leak compromised information.

Can you describe some of the actions taken during your missions?

As soon as a data leak is identified, the first step is to assess how recent it is. Is this newly exposed data, or is it recycled material that has already circulated online?

When possible, investigators will try to obtain a copy of the leaked dataset, taking strict precautions to avoid contamination. Files may be infected with malicious code.

If the source of the leak can be traced to a specific victim, cyber investigators contact the organization or individual involved to inform them and collect a formal complaint, along with any technical evidence that may help guide the investigation.

Then investigators work to gather proof and establishe the suspect's role in it. The goal is to stop the leak, support the victim in the reporting procedures, including notifications to authorities such as the CNIL (French data protection authority) or ANSSI (French national cybersecurity agency). When required, they can also identify the root cause of the compromise to prevent further intrusions, and track down and arrest those responsible and bring them to justice.

Several mechanisms are in place to support victims and raise awareness around cyber threats.

For professionals, particularly small and medium-sized businesses, platforms such as **17Cyber** provide immediate assistance if an attack occurs. They can also turn to **MonAideCyber,** designated security advisors, and dedicated cybersecurity audits to assess and improve their internal defense mechanisms.

Private individuals have access to a range of tools and services, including the **MaSécurité** mobile application, the government portal **Cybermalveillance.gouv.fr,** as well as reporting platforms such as **Pharos, Perceval, Thésée, and the digital brigade.**

Beyond institutional support, basic cybersecurity best practices can reduce the risks. This includes enabling two-factor authentication, keeping systems and applications up to date, receiving proper training in information security, limiting one's digital footprint, avoiding password reuse, and using password managers tools. It is also recommended to refer to the cybersecurity guide published by ANSSI which remains a key reference and offers practical guidance.

Credit photos : Unité Nationale Cyber

CREDITS

Editor-in-Chief : Arnaud LEROY
Graphic Design: : Arnaud LEROY
English Translation : Maëva ASTORGA
Magazine's mentor : Guillaume POUPARD

We would like to thank everyone who contributed to this issue.

January/March 2026

To support magazine