The Russian Cyberpunk. How the Kremlin Builds a Digital GULAG — And Who Is Resisting It

(Represented in the US under the title "Putin's Privacy on Sale. Inside the World's Biggest Data Black Market")

By Andrey Zakharov

This translated sample contains 3 chapters out of 10.

Volume: 50.000 words / 200 pages

Rights available for all languages except Russian and French.

Russian full manuscript available.

For all inquiries: *rights@straightforward.foundation*

Supported by the StraightForward Foundation.

OVERVIEW

“I’ll write her name down. You look at it and tell me if it’s her. Then I’ll tear it up right in front of you.”

“Andrei, they’ll kill me.”

It was autumn 2020. The two of us were tucked away at a corner table in a Moscow restaurant—me, a journalist with *Proekt*, an independent investigative outlet, and my companion, a former high-ranking official who had witnessed Vladimir Putin’s sharp rise through the ranks at the turn of the millennium.

I scribbled “Svetlana Krivonogikh” onto a page, tore it out, and slid it across the table.

“Andrei, they’ll kill me! I’m not saying a word,” he said, stroking his thick, chestnut-coloured beard with a nervous hand. That was all I needed. I tore the paper into small pieces and tucked them into my coat pocket.

By then, I had already pieced together a compelling trail of circumstantial evidence suggesting that Krivonogikh had once been Putin’s lover, that she had borne him an illegitimate daughter, and that she had grown wealthy thanks to gifts from the president’s close circle. The tremble in my source’s beard only confirmed I was on the right track.

“If Putin really had a daughter with Krivonogikh”—the surname literally means 'crooked-legged' in Russian—“then she must look like him,” I thought. I had to find her.

For such complex work, I had my secret weapon: a pirated disc containing a crude program where you could type in a full name, and it showed, for instance, who someone was registered to live with. In St Petersburg, Krivonogikh lived with a 17-year-old girl named

Elizaveta Rozova. Her patronymic—Vladimirovna—was another indirect clue that her father might be Vladimir Putin.

The trail ended on Rozova's *VKontakte* page (Russia's equivalent of Facebook). From the photos, Vladimir Putin was staring back at me—only this time, as a teenage girl.

#

In Russia, every piece of data can be bought—this means not only your passport or insurance number, but also information about your reservations, trips, food orders, taxes and everything else you can imagine. For years, the government has been attempting to put this market under its full control. So far, however, these attempts have been far from successful. While it's true that Putin's Russia is a digital surveillance state, it is also true that anyone with financial means and internet access can gain access to the most sensitive data of both ordinary and high-ranking people. Criminals use this information to create intricate scams, stalkers use it to follow their victims, and investigative journalists use it to uncover the state's darkest secrets.

In Putin's Privacy on Sale, I paint the full picture of this wild reality and make sense of what happens when data is set loose in a repressive society. The main characters of the book are people who created this reality: tech moguls (such as Pavel Durov, Telegram's founder), KGB agents, sellers of private information and others major players in the market of de-anonymization and surveillance in Russia. The book explains how the repressive and often careless attitude towards data and tech can bring the worst out in people but it can be turned to fight against those who are in power.

There are a few compelling frameworks that describe the digital age we live in. American philosopher Shoshana Zuboff calls it *surveillance capitalism*—a system in which corporations like Google and Meta, knowing almost everything about their users (that is, a significant portion of the world's population), hold unprecedented power. Greek economist Yanis Varoufakis offers a different lens: he calls our era *techno-feudalism*, where these same tech giants act as a kind of digital nobility. They rule over their domains with limited oversight from the "king"—the state—and extract rent from their serfs: the users. Both concepts reflect legitimate fears about the power of corporations that control vast troves of personal data and, in essence, monitor humanity. The key difference in Russia is this: while Google, Meta, or Amazon gather data to better monetize their users, the Kremlin seeks to collect data in order to control—and punish—them.

China is widely seen as the most prominent example of a state where technology is used effectively for population control. There, a vast network of facial recognition cameras is in operation, Western social networks and search engines are blocked, and a social credit system has been introduced—digital profiles built from government and private data to assess citizens' behavior (whether they repay loans, have been fined for drunk driving, gamble, or buy luxury goods). Russian authorities often look to China as a model, but so far, they've been unable to replicate it fully. One key reason is that in China, the internet came under state control right from the start: the so-called "Great Firewall" was put in place to filter all incoming traffic from the outside world. In contrast, Russia's communications networks were built with no government restrictions at first, and Western platforms and social media entered the domestic market freely.

All of this imposed technical, political, and commercial constraints on the Kremlin's attempts to build a Russian version of the "Great Firewall of China" after Putin began his third

presidential term in 2012. Here are two telling examples from the spring of 2025, as I'm finishing this book. First: Facebook and Instagram are officially banned in Russia, as their parent company, Meta, has been designated an "extremist organization." Yet another Meta product—the messaging app WhatsApp—not only continues to function without restriction but is officially listed among the top three most-used internet services in the country. Second: in Moscow, there's no escaping facial recognition cameras—they're installed at nearly every apartment entrance. But the moment you leave the capital, the situation changes entirely: across much of the country, the technology is scarcely used at all.

The Russian path—not the Chinese one—deserves close study by those concerned about their own countries sliding into authoritarianism. As in Russia, restrictions can be introduced gradually, sometimes even imperceptibly to civil society, under the guise of protecting the common good or upholding constitutional rights. One of the first moves made by Donald Trump's administration after his second return to the White House was to restrict journalists' access to the president. Previously, the list of accredited media outlets had been compiled by an independent association; now, it was drawn up by government officials. For American journalist Peter Baker, who once reported from Moscow, this echoed how the Kremlin gradually shut out critical reporters from the presidential press pool in the early 2000s, just as Putin was consolidating power. In France, in 2025, the parliament came close to passing a law that would have required encrypted messaging platforms—such as WhatsApp, Telegram, and Signal—to build in a backdoor for law enforcement, essentially enabling authorities to decrypt past communications. The proposal was justified as a tool in the fight against drug trafficking, but a backdoor renders any digital platform inherently vulnerable—it opens the door not just to state surveillance but also to hackers. All of this closely resembles Russia's "information

dissemination organizers" law: any social network, messenger, or online service included in a government-approved registry is obligated to provide encryption keys to the Russian security services. In essence, it's the same demand currently being floated by their French counterparts. So far, however, France has not adopted such a law—civil society had its say.

But a funny thing happened in Russia as it attempted to control citizens with data. Under the same "information dissemination organizers" law, refusal to cooperate with authorities should lead to a platform being blocked—just like Telegram was in 2018. At the end of 2024, WhatsApp was added to the official registry. There's no public evidence that Meta, which owns WhatsApp and has been designated an extremist organization in Russia, has complied with government demands. And yet, no one is blocking the country's most popular messenger—despite having every legal reason to do so. In fact, there are grounds for blocking it under other Russian laws as well, such as the ban on storing Russian citizens' personal data abroad. But the Damoclean sword of a ban, which has been hanging over WhatsApp for years, remains suspended. In Russian cyberpunk reality, that's not a contradiction—it's the norm.

Don't expect a perfect match with the world painted by sci-fi writers or cyberpunk filmmakers. In those dystopias, it's characters like Neo or the Blade runner who come out on top. In reality, the ending is still unwritten: the Kremlin is steadily building a hardline authoritarian system straight out of *1984*, while we—today's partisans, so to speak—resist it from exile, not from within Russia, where repression has forced us out. But the state hasn't won yet—and this book will show you why, for the same tools used to repress a population can also be turned against the oppressors. Just as leaders around the world are taking a page from Putin's playbook, so too can people learn from resistors who have become entrepreneurial about deploying data to

fight back. This is my story and the story of Russia today, but it is a guide for citizens in democracies sliding into authoritarianism.

ABOUT THE AUTHOR

Andrei Zakharov is a Russian digital and investigative journalist. Among his investigations he conducted are stories on how the owner of a notorious mercenary company called the Wagner Group, Yevgeniy Prigozhin, and his Internet Research Agency tried to interfere in the 2016 US elections. For the BBC, Zakharov investigated Moscow's state surveillance system and the Russian black data market. For the leading Russian investigative outlet Proekt, Zakharov worked on investigations about Putin's secret daughter and a historical film on Russian trolls and the first stages of the 2014 war with Ukraine.

In 2021, Russian authorities declared him a "foreign agent." After that, Zakharov faced an unprecedented level of surveillance and left Russia. In 2024, Russian authorities opened a criminal case against Zakharov and subsequently placed him on a wanted list.

Since the end of 2022, Zakharov has focused on his own media projects. Zakharov is the author of the book "Crypto. How Cypherpunks, Programmers and Rogues Bound Russia With Blockchain" (Individuum, 2023). In 2024, one of the book's protagonists, Kremlin-linked Orthodox oligarch Konstantin Malofeev, attempted to have the book's print run destroyed through a lawsuit in Russia. Zakharov started to work on the current book as a Fellow of Institute for Human Sciences fellow (IWM, Vienna). In 2024 he was named a Khlebnikov Russia Civil Society Fellow at the Harriman Institute at Columbia University.

Zakharov is currently based in Bulgaria.

SUMMARY OF CHAPTERS

Chapter 1. Putin's Secret Daughter

(*The main character in this chapter is the author, Andrey Zakharov*)

No later than the 2000s, Russian journalists began using leaked databases in their investigations. At that time, such databases could even be bought in the subway. When I started working at *Fontanka* in St. Petersburg, I began using them too — for example, I could check who someone had flown with.

In 2019, I did an investigation into the data-trading market, where one can buy almost any — and, most importantly, up-to-date — information about a person: who they called, where they live, what property they own, what tickets they bought. All this came from the databases of the Ministry of Internal Affairs, the Federal Tax Service, the Pension Fund, mobile operators, and banks. Unlike leaked databases, this was current information. I became an expert on this market, giving media interviews about it — while also using it myself. In 2020, I bought information on Putin's daughter from that market.

Later that year, the investigative journalism powerhouse Bellingcat admitted to using the same market, and to help readers understand what it was, they linked to my investigation. In the chapter, I will bring readers into the information underground demonstrating the tools of the trade as I embark on the highest profile investigation of my career.

Chapter 2. A Nerd with a Laptop

(*The main character in this chapter is Christo Grozev from BellingCa*t)

Christo Grozev, born in Plovdiv, studied in Luxembourg in his youth. During the collapse of socialism in Bulgaria, he broke into his country's embassy to retrieve secret documents. In the 1990s and 2000s, he lived in St. Petersburg and developed commercial radio stations, including *Eldoradio*. One of the people who signed the registration documents for his business was then-deputy mayor Vladimir Putin.

In the mid-2000s, Christo claims he was forced to sell his business in Russia and has harbored a grudge against the Russian authorities ever since. In 2014, he joined the Bellingcat team to find evidence of Russian presence in southeastern Ukraine and became the team's primary buyer of data from the leak market — including data on the Skripal and Navalny poisoners.

In 2022, he left Vienna, where he had been living, after intelligence services warned him that Russian authorities were planning to kill him.

Chapter 3. A Man from the Middle of Nowhere

(The main character in this chapter is the data seller from Chuvashia)

Among the data sellers (police officers, bureaucrats, and employees of banks or mobile providers) are anonymous brokers. One of them — an ordinary guy from Chuvashia named Ruslan G. — made hundreds of thousands of rubles monthly with a friend by selling data. It

turned out that he was the one who sold Christo Grozev the information about Navalny's poisoners, without knowing who he was or who Navalny even was.

When the investigation into the poisoners was published, the FSB quickly found Ruslan and his partner. The partner was arrested, and Ruslan, along with his mother, brother, and sister, escaped to Ukraine with Christo's help — despite rarely having left Chuvashia before. Christo later helped them relocate to Bulgaria, where I met and befriended him.

Chapter 4. The Citizen Surveillance System in Moscow.

(The main character in this chapter is the mayor of Moscow for the last 15 years, Sergey Sobyanin)

In 2011, the construction of the "Smart City" system began in Moscow. Technocrat Sergey Sobyanin visited Singapore and admired how data (and citizen surveillance) was used to govern the city-state. The architect of this "gulag" was Artem Yermolaev, a former manager at the Western company Cisco. Moscow started purchasing cellular data from telecom operators to understand how citizens move around the city — where they work and live. It built a transport management system that received real-time data from public transport, car-sharing services, and taxis, and learned to analyze Muscovites' behavior on the internet. By the time Yermolaev left city government in 2018, the mayor's office could use data to identify which apartments were being rented out and which were not.

In 2020, a facial recognition system using CCTV cameras was launched in Moscow. It involved four systems — three Russian and one Belarusian, the latter of which would later help

Lukashenko hunt opposition members. The most well-known was the system developed by NtechLab. Its founders became symbols of IT entrepreneurs who helped build a total surveillance state, treating their project as just an interesting business. One was PR man Alexander Kabakov, who had worked on Mikhail Prokhorov's campaign and for state companies, the other was programmer Artem Kuharenko. After the war began, they claimed to have sold their stakes in protest over the country's direction — though it was later revealed they had not. Their system helped authorities identify protesters in Moscow and later conscripts.

Chapter 5. SORM King

(Protagonist — "SORM King" Anton Cherepennikov)

In 1996, the SORM-1 system (an acronym for "system of technical means for ensuring the functions of operational-search activities") was launched, allowing for wiretapping of suspects' phones. In 2000, SORM-2 was introduced to capture internet traffic. While similar systems exist in the West, intelligence services there require court approval to access data. The FSB, however, was allowed to monitor traffic without any such approval.

The main supplier of this equipment — the so-called "SORM king" — became young entrepreneur Anton Cherepennikov. He started out in esports, owning a team while also supplying SORM hardware. He then met Alisher Usmanov, who initially funded his esports venture and later used him as a business proxy for SORM equipment distribution. Cherepennikov became a billionaire through his ties to security services, while also investing in

cybersecurity startups, posing as a venture capitalist. One such startup belonged to the son of FSB deputy chief Sergey Korolev.

In 2016, Russia passed the "Yarovaya Law," requiring telecom operators to store users' texts, voice and video messages (SORM-3). Debates followed about how long data should be stored, as Russia lacked the storage infrastructure. By 2018, it was decided that data would be kept for six months.

In 2023, Cherepennikov died under mysterious circumstances — reportedly after undergoing xenon therapy, a popular rejuvenation treatment among security officers.

Chapter 6. The Total Internet Blocking System

(*Protagonists — "Orthodox Telecom Officer" Igor Shchyogolev and Sovereign Internet Law Author Andrei Lipov*)

For a long time, Russia's main censorship body, Roskomnadzor, blocked websites by IP. In 2018, it attempted to block a powerful service — Telegram — and lost. Telegram's founder Pavel Durov rented millions of IP addresses; Roskomnadzor blocked them, disrupting unrelated services, but Telegram kept working.

After this failure, Roskomnadzor adopted new tech: DPI (deep packet inspection), which identifies traffic patterns unique to specific services. DPI hardware was deployed at government expense by the Usmanov-Cherepennikov company. The project was completed by Roskomnadzor's new head, Andrei Lipov, who also authored the "Sovereign Internet" law and came from Orthodox circles.

In 2021, the first real test of this equipment was the throttling of Twitter. After the war began, opposition news sites and Western social media (except YouTube) were successfully blocked. Russia continued to purchase DPI equipment from abroad. In autumn 2023, Lipov announced that 100% of networks were equipped with the new system, and Roskomnadzor began testing it on VPN protocols.

Chapter 7. Creator of the "Eye of God" Telegram Bot Yevgeny Antipov and Other Personal Data Aggregators

In the USSR, the 5th Directorate of the KGB was responsible for citizen control and managing ideology. Vladimir Putin began his KGB service there. It was so focused on control that it even had a department for tracking anonymous letter writers to the press and government. In the late 1980s, a monumental computing center was built near Lubyanka (now the FSB Information Security Center). Around then, the KGB developed a GUI for personal data databases (addresses, phone numbers). In the early '90s, after the USSR collapsed, KGB veterans commercialized this tool as "Kronos."

For 20 years, Kronos served as the main interface for working with leaked personal databases sold at Moscow radio markets. These included address books, phone directories, business registries, police and real estate data — even gangster contact books. Some databases contained evidence of criminal pasts of people who later tried to hide it. Another, called "Sirena," tracked air travel — including trips by Putin and his alleged lover Svetlana Krivonogikh in the late '90s.

Users of Kronos included investigative journalists (screenshots appear in early Navalny exposés), bank security, private detectives — possibly even law enforcement. Other early aggregators: Larix and the "Moscow Center for Economic Security."

By 2020, a group called Da Vinci began buying up leaked databases and, at the end of the year, launched the first Telegram data lookup bot — enter a name or phone number and get detailed personal data for a small fee.

In 2021, bloggers tracked the bot's creator through payment data: programmer Yevgeny Antipov, who started with ICQ bots, lived in Portugal, then returned to Russia. Despite a search of his home, he was not arrested. The bot continued operating — Roskomnadzor demanded Telegram delete it, Telegram complied, but Antipov simply relaunched it under a new name. He gave interviews claiming that since the data had already leaked, he wasn't violating the law. The bot later offered expanded access for police. By 2022, it was being used to identify Telegram commenters critical of the government. At that point, Roskomnadzor stopped attacking it. The chapter illustrates the importance of aggregators. Data becomes useful information when you create a user-friendly interface.

Chapter 8. Data "Lookups" Spread Across the Country

In the chapter, I will portray the rise of data lookup services and what it means when anyone can find anyone. One man, Ivan, kept tabs on his ex for years, buying her billing data, travel records (he showed up at her vacation spot), and current addresses via bots. He even installed a tracker

under her mother's car. He learned from Navalny's investigations — and admitted to using others too. Eventually, he was sentenced to community service for purchasing personal data.

People commonly use lookup services to find family or for other personal reasons. It is a tool of journalists as well as political actors. In 2020, a Moscow court sentenced a group for hacking the phone of Foreign Minister Lavrov's billionaire son-in-law, Alexander Vinokurov. Hackers got his billing and WhatsApp data. Authorities tracked the entire chain — from telecom insider to Telegram data seller to the client. The client turned out to be Alexander Maloletko, linked to Wagner PMC. He was fined.

In 2022, "Putin's chef" Prigozhin posted a photo of himself with Maloletko at a Wagnerite's grave. When asked if it was the same man convicted for the Lavrov hack, Prigozhin said yes — but called the verdict unfair.

Chapter 9. Fake Call Centers — Russian and Ukrainian Fraudsters and Their Victims

Black market data wasn't used only by journalists or jealous exes. In the late 2010s, Russians were plagued by scam calls from fake "Sberbank" call centers, often located in prisons or Ukraine. Fraudsters used leaked databases to call people by name and impersonate banks. At one point, Sberbank reported that one in three colonies had a fake call center.

The fake call centers did more than scam people. After the war began, Ukrainians began using similar tactics — using social engineering to convince Russian pensioners to commit arson against military enlistment offices.

Chapter 10. VK

(*Protagonist — Pavel Durov*)

During the 2011 election protests, police came to “VKontakte” director Pavel Durov. Refusing to open the door, he texted his brother and realized the police could read their messages in real-time. This, he later said, inspired him to create Telegram.

He worked on Telegram intensively after selling VK to Alisher Usmanov. However, developers of both platforms had long worked side-by-side in the Singer House on Nevsky Prospect, fueling rumors that Usmanov had a stake in Telegram — rumors never proven.

Durov made Telegram a media platform with two key features: anonymous publishing and direct-to-phone delivery. He only removes or restricts channels under heavy pressure from local authorities (Russia, Germany). But Russian authorities have leverage: the TON project team is Russian, and financial services in Telegram are developed by Kazan entrepreneur Dmitry Yeremeyev.

By 2022, Telegram channels became major information hubs for both sides of the war — Ukrainian military and z-channels, as well as Russian politicians who migrated to Telegram after Western platforms like Instagram were blocked.

Chapter 11. Kovalchuk as Putin’s Consigliere, Managing the Most Popular Social Networks and Holding the Data of Hundreds of Millions of Russians

Yury Kovalchuk, known as Vladimir Putin's personal banker and consigliere, has become one of the most powerful and least visible figures in Russia's information control apparatus. His rise began in the early 1990s when, through a network of former KGB associates, he took over the obscure "Rossiya" Bank in St. Petersburg. As Putin transitioned from deputy mayor to president, Kovalchuk became his trusted handler of sensitive financial matters — from managing the assets of Putin's alleged family members to bankrolling the president's private residences. But Kovalchuk's influence extended far beyond finance: he was tasked with consolidating media control after Putin witnessed firsthand the political power of television during the 2000 election.

Kovalchuk's media empire grew through a series of strategic takeovers and state-supported acquisitions, turning his network into a key instrument of Kremlin propaganda. With backing from Gazprom and political protection, Kovalchuk gained control over major media outlets, often using trusted proxies and shell companies. By 2025, he controlled or influenced five of the ten most visited websites in Russia, alongside a dominant share of national TV channels.

This expansion allowed the Kremlin to fuse state messaging with digital surveillance, particularly as the government pushed to replace Western platforms like YouTube. Kovalchuk's platforms became central to government propaganda campaigns, including the promotion of military service, which even appeared in school and kindergarten groups. His relatives were appointed to senior roles across his media holdings, reinforcing the feudal structure of Russia's information control. Despite massive state subsidies and aggressive suppression of alternatives, the attempt to build a "sovereign internet" remained fraught — with platforms like VK suffering financial losses and failing to rival the reach or credibility of their Western counterparts. Still, with Putin's blessing, Kovalchuk remains at the core of Russia's digital autocracy.

Chapter 12. The Russia–Ukraine Cyberwar

(*Protagonist — Anonymous Hacker*)

In 2022, not only did a conventional war begin between Russia and Ukraine, but also a cyberwar. Ukraine's IT Army — a volunteer hacker community — launched DDoS attacks on government, corporate, and media websites. As a result, 2022–2023 saw record personal data leaks of Russian citizens — from schools, post offices, banks, clinics, and e-commerce platforms.

These leaks contain enough information to create a digital profile of nearly every Russian citizen. Some Telegram bots use only this data.

There were also sensitive leaks of Ukrainian data — a "response" from Russian hackers, often tied to security agencies.

Epilogue

I return to the investigation that led to identifying Putin's illegitimate daughter. The state is trying to replace cyberpunk with a "digital GULAG": closing off public data (like Rosreestr), and planning to deploy facial recognition across the country. Governments worldwide are moving in the same direction. How can civil society counter this trend?

Chapter 1: Putin's Secret Daughter

“I’ll write her name down. You look at it and tell me if it’s her. Then I’ll tear it up right in front of you.”

“Andrei, they’ll kill me.”

It was autumn 2020. The two of us were tucked away at a corner table in a Moscow restaurant—me, a journalist with *Proekt*, an independent investigative outlet, and my companion, a former high-ranking official who had witnessed Vladimir Putin’s sharp rise through the ranks at the turn of the millennium.

I scribbled “Svetlana Krivonogikh” onto a page, tore it out, and slid it across the table.

“Andrei, they’ll kill me! I’m not saying a word,” he said, stroking his thick, chestnut-coloured beard with a nervous hand. That was all I needed. I tore the paper into small pieces and tucked them into my coat pocket.

By then, I had already pieced together a compelling trail of circumstantial evidence suggesting that Krivonogikh had once been Putin’s lover, that she had borne him an illegitimate daughter, and that she had grown wealthy thanks to gifts from the president’s close circle. The tremble in my source’s beard only confirmed I was on the right track.

“If Putin really had a daughter with Krivonogikh”—the surname literally means 'crooked-legged' in Russian—“then she must look like him,” I thought. I had to find her.

For such complex work, I had my secret weapon: a pirated disc containing a crude program where you could type in a full name, and it showed, for instance, who someone was registered to live with. In St Petersburg, Krivonogikh lived with a 17-year-old girl named Elizaveta Rozova. Her patronymic—Vladimirovna—was another indirect clue that her father

might be Vladimir Putin. The trail ended on Rozova's *VKontakte* page (Russia's equivalent of Facebook). From the photos, Vladimir Putin was staring back at me—only this time, as a teenage girl.

I messaged the photos to my editor, Roman Badanin. "F*ck!" he wrote back. Five minutes later: "F*ck me. F*ck me sideways." And that's how my trusty helper—a bootleg disc of personal data I had quietly assembled over years—brought me to the biggest investigation of my career.

Agency "The Detective"

In the early 1990s, a book series called *Children's Detective* appeared in the bookshops of my hometown—a city that had only recently been renamed St Petersburg, reclaiming its original name after decades as Leningrad under Soviet rule. The series was made up of translated Western novels, part of the wave that flooded into Russia after the collapse of the USSR and the fall of the Iron Curtain. Each cover featured the profile of a pensive boy, finger pressed thoughtfully to his chin. These were the books' heroes—boys, and occasionally girls—who, despite their age, managed to catch real criminals somewhere in the US or Britain, then pedalled off to a carefree countryside picnic. I had a bike too—just a *Shkolnik (*"Schoolboy"*)*, the plain Soviet model—but I couldn't boast of having solved any crimes myself. Not yet.

To test my investigative skills, I needed real mysteries to solve. I cut up little rectangles of paper and stamped them using special rubber stamps: *Agency "The Detective"* and our home phone number. I slipped the business cards into neighbours' mailboxes and waited for my first client. When no one came, I took to the streets in search of secrets. In one courtyard, I was drawn to a Soviet-made Moskvich—a squat, domestic-brand car—with a model crown stuck to its

dashboard. Trinkets like that were a common bit of flair back then. But to me, the crown looked real. “Stolen from a museum!” I hypothesised, like a proper detective. I stared into the car’s interior for so long, trying to find some kind of evidence, that the owner—watching from a balcony above—suddenly shouted at me, clearly thinking I was a thief. And who could blame him? In the early ’90s, street crime had become so common that people would often take their car stereos indoors for the night, just to stop someone smashing the window to steal them.

Ten years passed. It was a hot, stifling summer in St Petersburg. I was a university student, riding the metro on my way to an exam. A man in a T-shirt and a grey vest—the kind with a dozen pockets across the chest—shuffled through the carriage. “Telephone database of St Petersburg residents, licence plate database,” he muttered, holding a stack of homeburned discs in one hand and dabbing the sweat from his neck with a handkerchief in the other. I suddenly remembered my old agency, ″The Detective", and thought: if I’d had access to a database like that back then, I would’ve started my “investigation into the mysterious crown” by checking who owned that Moskvich. “150 rubles a disc,” the man said, waving the handkerchief in front of my face. I turned away. Back then, 150 rubles was the price of lunch at a student canteen—and in that moment, I didn’t need any databases.

Back then, discs with personal data weren’t just sold on the metro. You could find them in underground passages, at street markets selling cheap clothes—and, of course, online. In 2005, a reporter for *Rossiyskaya Gazeta*, the Russian government’s official newspaper, spotted an ad on the internet: a database for sale containing mobile phone numbers, addresses, and passport details of residents of Khabarovsk, a city in the Russian Far East. The deal went down in a lecture hall at a local university. The seller handed over the disc, took the cash, and vanished.[1]

[1] Cellular companies' customer databases are freely available for sale // https://rg.ru/2005/12/09/telefon-baza.html

Inside the database, the journalist found himself, his friends, local officials—and the head of the Khabarovsk branch of the FSB, Russia's main security agency and successor to the Soviet KGB.

Around the same time, a correspondent for the St Petersburg edition of *Kommersant*—one of Russia's leading business newspapers—bought a database containing every mobile number in the city as part of a journalistic experiment. Two men delivered the discs. One handled the technical side; the other acted as his bodyguard and handled the legal talk. While the tech guy was installing the database on the computer, his partner explained why he wasn't worried about getting into trouble for such a shady enterprise: "We can always find a common language with the regular cops. And besides, there are no legal grounds for arrest—nobody's copyright is being infringed."[2] The journalist opened the database and began calling local celebrities. The numbers were real, of course—every single one. The discs, which contained nearly five million phone numbers from St Petersburg and the surrounding region, cost about $50 (here and elsewhere, currency conversions reflect the exchange rate at the time).

By the mid-2000s, Russians' personal data was, quite literally, lying around for anyone to grab. "Almost every stall selling CD-ROMs had a sign reading 'Latest databases'," recalled another journalist, describing his trip to the radio market in Moscow's Mitino district.[3] "When you asked, 'What's new?' the sellers would silently hand you a thick catalogue listing the full selection and prices."

The fact that addresses and phone numbers were being traded like snacks at a street stall could be chalked up to the absence of any law protecting citizens' digital information. Eventually, the authorities began to realise that something had to be done. "Everyone knows full

[2] Quite a number: The Databases of All Mobile Operators Were Stolen in St. Petersburg // https://www.kommersant.ru/doc/382755

[3] Peepers: Today it is possible to find out any information about Russian citizens. The question is the price // https://web.archive.org/web/20051118193753/http://versiasovsek.ru/material.php?3990

well that some databases can be bought right on Tverskaya Street [in central Moscow],” Information Technology Minister Leonid Reiman told the State Duma in November 2005. “So, to prevent this from happening, we’re planning to create a whole set of mechanisms—legal, legislative—to put a stop to this negative phenomenon.” He was presenting the draft of a new law: *On Personal Data*.

The law passed—but the databases didn’t vanish from open sale. Just a few months after the new regulations came into effect, a disc turned up at the radio market in Moscow’s Mitino district. It contained data on three million borrowers who had ended up on Russian banks’ internal blacklists. For just $60, you could find out their names, addresses, phone numbers, places of work—and the reasons they were considered unreliable loan recipients. Sometimes it was as serious as a criminal record.[4]

Of course, large-scale personal data leaks have happened in every country. In that same year—2006—the United States was dealing with the possibility that the personal data of more than 26 million military veterans[5] had fallen into the wrong hands. In Britain, there was the theft of records on 11 million members of the Nationwide Building Society, a kind of mortgage bank.[6] But in the West, even the worst of these databases might end up on some closed, specialist forum—not sold openly on a disc from a market stall near the Houses of Parliament, while the minister in charge and a roomful of MPs discuss how to crack down on leaks.

In the summer of 2008, a man selling discs with mobile operator databases stepped into a metro carriage in St Petersburg. One of the passengers, a 59-year-old man, pointed out that it was

[4] Data leaks // https://www.kinnet.ru/cterra/679/311807.html
[5] Personal Data of 26.5 Million Veterans Stolen // https://www.nytimes.com/2006/05/22/washington/22cnd-identity.html
[6] Nationwide fined £1m over laptop theft security breach // https://www.theguardian.com/money/2007/feb/15/business.accounts

illegal to sell such data in public. In response, the vendor punched him in the eye and jumped out at the next station. The passenger had to call an ambulance.[7]

His outrage was understandable. Databases had become a dangerous weapon in the hands of criminals. In St Petersburg, for example, a gang of car thieves used a leaked traffic police database to forge documents for stolen vehicles—inserting real chassis and engine numbers to make them look legitimate. In Moscow, fraudsters armed themselves with a leaked file of medical records and began cold-calling people, offering tinted water and crushed chalk as miracle cures. The phone numbers, of course, came from another database.[8] Later, these leaked datasets would become the foundation for fake bank call centres. Scammers, calling directly from prison colonies, used psychological tricks to pressure citizens into voluntarily transferring their entire savings. The power of the scheme lay in the details: names of relatives, property records, even bits of real personal history—all pulled from stolen databases—made the fraudsters seem trustworthy enough to believe.

Journalists were also active users of leaked databases. In 2005, for example, reporters at *Vedomosti* discovered detailed information in a leak of Central Bank wire records about how the state-owned oil giant Rosneft had used a clever scheme to take over the oil business of Mikhail Khodorkovsky—a politically sidelined billionaire who had openly challenged Vladimir Putin and funded the Russian opposition, but who ultimately lost his major assets and ended up in prison.[9]

A few years later, I finally had a reason to use those leaked database discs myself.

---

[7] The seller of stolen phone bases in the metro beat up a passenger // https://konkretno.ru/lenta_an_op/11364-prodavec_vorovannykh_telefonnykh_baz_v_metro_izbil_passazhira.html

[8] Data leak surge // https://ecm-journal.ru/material/Slivnojj-skachok

[9] What is the secret scheme for financing the purchase of Yuganskneftegaz? // https://neftegaz.ru/news/companies/299729-kakova-sekretnaya-skhema-finansirovaniya-pokupki-yuganskneftegaza/

At Vasily’s

“You flew with him to Adler.”

“How do you know that?”

“You were seen in the neighbouring seats.”

“By whom?”

“I can’t reveal the source.”

The questions in that conversation were asked by an official from the St Petersburg city administration—and I was the one answering them. These were the kinds of exchanges I had once dreamed of, back when I was stamping business cards for my agency "The Detective". That dream came true at the end of 2010, when I began working at the St Petersburg Agency for Investigative Journalism—whose main project was, and still is, the online publication *Fontanka.ru*.

Our editors always demanded that we publish the news faster than our competitors—which meant we had to dig deeper, uncover more, get there first. Sources inside government or the security services often helped with this. But first of all, they didn’t always have the information you needed. And even if they did have “tips from an insider,” they took their time before sharing any secrets. Second, there was the risk of becoming dependent on a source. After all, if someone did you a favour, they expected something in return—like asking you to give an event they cared about a "quiet media push". In that sense, the leaked databases turned out to be the most selfless and unfailing partner—the kind that would hand you the mobile number of whatever businessman you needed, or quietly lay out the relatives of a corrupt official.

When I started working at *Fontanka*, I often thought back to that metro vendor selling discs full of phone numbers—and I already regretted not buying one back then. But soon I gained access to a system that had gathered hundreds of leaked databases—all searchable at once. I won't say how I found out about it, or who gave me the remote access keys. That's not my secret to tell, and revealing it—even years later—could hurt people I care about. I'm not even sure I can mention its real name, so I'll just call it *The Base*. Later, I learned there were several similar aggregators in Russia. Most of them were more or less alike, but ours had one key advantage.

The Base was regularly updated with fresh data from the Ministry of Internal Affairs' internal system, *Rozysk-Magistral*. That system automatically logs every ticket purchased by Russian citizens for planes—including international flights—as well as trains and long-distance buses. Other aggregators had only patchy travel data, mostly from leaks dating back to the early 2000s. But *The Base* offered the most up-to-date records—including information on what it called "travel companions." That's what the system named people whose tickets were purchased at the same time, down to the minute. If two people buy their tickets together—whether at a station or online—the logic went, they must know each other.

It was a killer tool for uncovering the social circle around your investigation target—whether an official, a businessman, or a criminal. Take Andrei Bondarchuk, head of the St Petersburg government's energy committee—the same one who once asked me who had supposedly seen him on the plane. *The Base* helped me identify a man who'd received preferential treatment from Bondarchuk's department—and who had flown with him to Adler. When I asked the official about his seatmate, he muttered something along the lines of, "I've got acquaintances practically everywhere." The story I published about him became another strong

addition to my growing portfolio of anti-corruption investigations at *Fontanka*. By the end of 2016, that portfolio had thickened, and I was invited to work in Moscow—as a special correspondent for the independent business magazine *RBC*. It was a step forward in my career as a journalist, but it came with a cost: I lost access to *The Base*. My connection to that magic system had been tied to my old job. I wasn't used to investigating without leaks anymore—and not long after arriving in Moscow, I found myself heading to one of the city's radio markets in search of discs.

The market turned out to be just an ordinary shopping centre, filled with an endless sprawl of shops mostly selling phones and laptops. "Hey man, just say what you need," vendors kept calling out, trying to draw me in. I must have heard that line dozens of times before I finally stumbled across a little booth with a sign that read: SIM cards, discs, databases**.** Inside sat a tired, unshaven man in his forties—phlegmatic, barely interested. His entire shop was a cubicle no larger than two metres by one and a half, with just a computer and a space heater.

When I asked if he had any databases, the man glanced up from his computer, where a primitive game was frozen on the screen. He looked at me with suspicion and asked who I was. "I'm a journalist. I work for RBC—you know the media holding?" That changed everything. He perked up, smiled, and started boasting that colleagues from other outlets dropped by all the time. He named a couple of investigative reporters he knew from liberal newspapers, though most of his regulars were crime reporters from television. Vasily—not his real name—clearly took pride in the fact that correspondents from the country's top TV channels came to him. He didn't ask for any credentials to prove I was really a journalist—my word was enough for him to promise me several popular databases. All I needed was an empty external hard drive. When I asked about the price, Vasily just shrugged and said he "likes helping journalists for free."

When I came back the next day with the hard drive, Vasily left me alone in his little cubicle and disappeared somewhere—as I later realised, he didn't keep any databases on-site. Ten minutes later, he returned and told me he'd loaded a database of Moscow residents with addresses, a fresh traffic police database with drivers' mobile numbers, and "a few other bits and pieces." The Moscow address database wasn't exactly up-to-date—it was from 2012, and this was 2017—but you have to start somewhere.

I got into the habit of dropping by Vasily's booth every so often to pick up new leaks. Once, I paid him around $100, but in most cases, he refused to take any money. We struck up a sort of friendship. I'd swing by, and he'd give me a quick two- or three-word summary of the latest leaks, then drift into stories from his life—tales about his family and complaints about the police who extorted him from time to time. When he stepped out to copy the files for me, I'd casually tell anyone who wandered up that Vasily would be back soon. One day—about a year after we met—he asked me to "go walk around for an hour." I wandered the market for a bit, and when I came back, he handed me a disc and said, "I copied everything for you."

That "everything" turned out to be more than a thousand databases, totalling nearly a terabyte and a half of data. The oldest leaks dated back to the late 1990s; the most recent had only just surfaced. Among them were databases containing the personal data of citizens of Ukraine, Kazakhstan, Belarus, and Moldova—in other words, most of the post-Soviet states. I kept that magic disc—encrypted, of course—hidden in the most secret corners of my home. I took it with me on every trip, and I brought it along when I was forced to leave Russia in the autumn of 2021, along with my laptop, a change of underwear, and a photo of my family.

Vasily's databases run on a system called *Cronos*. Like *Fontanka's* own *Base*, it's a shell program designed to let you search inside leaks by name, address, phone number, or other

identifiers. I launch the disc, open up a clunky, Windows-style interface straight out of the mid-1990s, and type a name into the search bar—for example, Vladimir Putin's former mistress: *Krivonogikh, Svetlana Vladimirovna***.** Up comes an old St Petersburg registration in a communal apartment in the city centre. Then a luxury flat nearby—purchased after the birth of her daughter by the president. Air travel records from the late 1990s and early 2000s. The most recent leak shows that in early January 1999, just after the New Year holidays, Putin boarded a plane at Pulkovo Airport in St Petersburg to return to Moscow for work—at the time, he was serving as director of the FSB, Russia's main security agency. Seated next to him, in the fifth row, was his bodyguard Viktor Zolotov. And up front, in the first row, sat Krivonogikh. The two had clearly taken precautions: the future president and his companion had purchased their tickets eight minutes apart.

Even if there's nothing in the database for the person you're searching, the name of the database still appears. I can't list all the thousands of entries, so here's a random sample:

Moscow. Ambulance Calls. 2012

Russian Standard Bank. Borrower Evaluations. 2013

Perm. Pension Fund. 2017

Saratov. Federal Drug Control Service—Operational Register. 2016

Arkhangelsk. Bank Debtors. 2014

Yekaterinburg. Drug Addicts. 2013

Russia. Photo Archive of Paedophiles. 2012

Syzran. Members of Organised Crime Groups. 2004

Irkutsk. HIV. 2013

Ufa. Drug Addicts. 2016

Samara. Brothels. 2011

Ukraine. Lviv. Drug Addicts—Special Watchlist. 2009

Kazakhstan. Convicted Individuals. 2003

Dates and places of birth, home addresses, criminal records, employment histories, salaries, real estate, vehicles, medical diagnoses—all of it. The leaks included databases from municipal and law enforcement agencies, hospitals, addiction clinics and insurance providers, election commissions, mobile operators, banks, and online retailers. Over time, working with the disc I got from Vasily, I came up with a rule of thumb: if someone doesn't show up in any of these databases, they either never lived in Russia, or arrived only recently and their data simply hasn't leaked yet. In all other cases, they had to have left some kind of digital trace. The real question was how to use that digital footprint in an investigation—because, strictly speaking, relying on leaked data meant crossing a line. It violated fundamental journalistic standards.

The *Mayak* Controversy

In May 2019, *Mayak*—a closed-door conference of Russian investigative journalists—was held in Riga. It was the first event I could remember where the ethics of buying and using leaked personal data were seriously debated.

Ivan Kolpakov, editor-in-chief of *Meduza*, wearing stylish cropped trousers and a loose white shirt untucked, was firm: "This is a violation of journalistic standards. It's unacceptable to purchase personal data—even if it's already been leaked." Roman Dobrokhotov, editor-in-chief of the investigative outlet *The Insider*, in his signature three-piece suit, calmly replied that he saw nothing wrong with the practice—especially when the investigation serves a clear public

interest. I limited myself to a few vague, noncommittal phrases—and didn't admit that, back in my hotel room, I had a disc from Vasily with a couple of thousand leaked databases on it.

The ethical conflict around using leaked data came down to a core principle of journalism: a reporter is not supposed to buy information from a source or subject. In some cases, that's barely distinguishable from a bribe—especially when the source is a government official or a police officer. Alongside that rule, every journalistic code also includes the basic requirement not to break the law. And using databases of unclear origin could, at least in theory, fall under several articles of the criminal code. "Is it true you're buying data on your subjects?" a *New York Times* reporter asked me in February 2021. I gave an answer so incoherent it didn't even make it into his piece on investigative journalism in Russia.

Neither I nor most of my colleagues made a habit of advertising the fact that we searched for our subjects in leaked databases. That kind of material was raw input for our work—but it was never the whole picture. Ideally, the data needed to be legitimised. For example, in 2020, during an investigation into Patriarch Kirill's luxury real estate, I reported on an apartment in central St Petersburg that had been gifted to one of his close relatives by a mysterious Swiss citizen. In the article, I cited publicly available records from the State Real Estate Register (Rosreestr). But in truth, I first discovered the property by typing that relative's name into Vasily's database.

Another way to legitimise information from leaks is to speak directly with the subjects—and cleverly coax them into confirming what you already know from the databases. That's exactly what I did, for example, when preparing an investigation into St Petersburg official Andrei Bondarchuk: I asked him casually about his neighbour on a flight from St Petersburg to Adler. And in early 2019, Russian business media were asking who really owned

the new general contractor for Gazprom—another state-owned corporation, and the country's monopoly in gas production and exports. According to the corporate registry, the stake in the company—which was set to manage up to $15 billion annually—was registered to an unknown individual named Sergei Furin. I ran his name through the leaked databases and found out he was just an ordinary driver. For instance, data from the leaked Moscow parking system showed that during working hours he drove a city minibus, and in his spare time, a modest 2008 Ford Focus.

The passengers on his minibus turned out to be... interesting people. I won't bore you with the complex schemes—suffice it to say, the tangled trail eventually led to Alexei Miller, the head of Gazprom. Which meant that, setting aside all formalities, Miller was effectively one of the co-owners of Gazprom's new super-contractor—a textbook case of conflict of interest. But how could I prove that Furin really was just a driver? I called one of his regular passengers and started by asking whether a chauffeur named Furin worked for him. He said yes—clearly caught off guard—but quickly went on the offensive, demanding to know how I'd gotten his number. I'd found it in one of the leaked databases, of course, but I still couldn't cite that. So I got creative again: I told him the number had come from some of his "acquaintances."[10]

Leaked databases were treated a bit more casually at the Anti-Corruption Foundation (FBK), the organisation founded by opposition politician Alexei Navalny. And that's entirely understandable: while the FBK carried out investigations, it was always a political organisation first—and Navalny's team didn't share the ethical hesitations typical of journalists. The Foundation was among the first to openly publish screenshots from leaks—often from the very same sources I relied on. In 2019, for example, while reporting on the connection between the

[10] How an ordinary Muscovite became Gazprom's business partner // https://www.bbc.com/russian/features-48423681

family of a high-ranking FSB officer and the funeral services business, Navalny's team posted a screenshot from the Moscow traffic police database.[11]

"We understood that the public interest was on our side. If the state shuts down access to data and makes it impossible to investigate its own actions, then our job is to use every tool available," Georgy Alburov, one of the FBK's investigators, told me. Alburov treated leaked databases much like pirated films: in the 2000s, you could buy them openly at street markets and underpasses; by the 2010s, you could simply download them online. A telling detail: FBK stored many of these databases on discs in their office. When the police raided the foundation, they seized the computers—but among the long list of criminal charges against Navalny and his team, ranging from "involving minors in protests" to terrorism and extremism, there was nothing related to the illegal use of personal data.

Ethical conflicts are even more complicated in stories such as the investigation into Putin's mistress Svetlana Krivonogikh. She became a billionaire thanks to her relationship with the president, receiving gifts from his friends — so public interest seems to allow breaking the law and standards and buying her personal data on the black market. But what about the head of state's illegitimate daughter? Where does public interest end and invasion of the privacy of a teenager who did not choose who her father is begin? In The Project, we resolved this conflict as follows: the focus of the material was on Krivonogikh, we did not mention the daughter's name, we did not publish photos of the girl, but we used her resemblance to Putin as one of the pieces of evidence of Krivonogikh's connection to the president.

If you set ethics aside and look at leaked databases purely from an investigative point of view, they all shared one major flaw: the information was rarely up to date. Even in the powerful *Base* I used at *Fontanka*, the data was incomplete and often arrived with a delay. Take my 2019

[11] https://navalny.com/p/6152/

investigation into Sergei Furin—the minibus driver who turned out to be the co-owner of Gazprom's biggest contractor. The most recent address data I could find in the leaks dated back to 2016. So I couldn't say with certainty whether he was still officially registered at that same unremarkable five-storey apartment block in a residential district on the outskirts of Moscow.

The most up-to-date and comprehensive information came from what's known as the "probiv" market—a black-market service that, sometimes for a hefty fee, gives you real-time access to the internal systems of police departments, banks, and mobile operators.

Bulgarian Footprint

In the spring of 2018, former Russian military intelligence (GRU) colonel Sergei Skripal and his daughter were found unconscious on a park bench in the English town of Salisbury. British investigators soon determined that the Skripals had been the target of a poisoning attempt—and not with just any toxin, but with a genuine chemical warfare agent.

In the 1990s, while holding senior positions within Russia's military intelligence service (GRU), Skripal began secretly cooperating with British authorities, supplying them for years with sensitive information—including the names of Russian agents operating abroad. He was eventually exposed, imprisoned, and in 2010 was part of a spy swap for Russian intelligence operatives who had been caught in the West. Given the grudge the Russian state held against Skripal, the most obvious suspects in the attempted assassination were, naturally, Russian intelligence services.

Six months after the attempted murder of the Skripals, investigators released the names under which the suspected poisoners had entered the UK, linked them to the GRU, and published their photographs: "Alexander Boshirov," sporting a mop of hair and a goatee; and "Ruslan Petrov," close-cropped and slightly unshaven. CCTV footage from Salisbury showed them

arriving by train from London, wandering near the Skripals' house, then heading straight back to the capital and flying to Moscow that same night. President Putin soon publicly confirmed that the two men were indeed Russian citizens—but insisted they had no ties to the intelligence services. The day after his statement, "Boshirov" and "Petrov" gave a televised interview to Margarita Simonyan, head of the Kremlin's main propaganda outlet, the Russian state channel *RT* (formerly *Russia Today*).

"Do you work for the GRU?" she asked.

"Do *you* work for the GRU?" Boshirov shot back, answering a question with a question.

"I don't. And you?" Simonyan repeated.

"Nor do I," the men replied, one after the other.

They introduced themselves as entrepreneurs in the sports nutrition business and claimed they had travelled to Salisbury as tourists—to admire the cathedral with its 123-metre spire and "the very first clock ever invented in the world." Their interview with Simonyan left a distinctly odd impression. It felt staged—but you can't build a story on impressions alone.

Just a couple of weeks after the Russia Today interview aired, the investigative group Bellingcat, in collaboration with *The Insider*, published a series of reports revealing that "Boshirov" and "Petrov" were in fact GRU officers who had entered the UK on false documents. The publications included screenshots from Rospasport, the Interior Ministry's internal passport database. Visually, the men in the screenshots were the same—only the names had changed. One of them had received his first passport as a teenager under the name Anatoly Chepiga, and later held another document as Alexander Petrov. The other, Alexander Mishkin, acquired an ID as an adult under the alias Ruslan Petrov. Leaked databases showed that one of them was registered in Moscow at the actual GRU headquarters. That address would later serve repeatedly as proof that

yet another compromised agent belonged to Russian military intelligence. Perhaps the GRU registered its personnel there for the sake of secrecy—but in a country where anyone can buy a leak-filled disc at a radio market, this habit turned out to be a colossal own goal.

Everything from the leaked databases checked out—I cross-referenced the findings on my disc, and it all matched. But I didn't have the Rospasport data. So I went back to Vasily at the radio market to ask whether he'd got hold of this latest leak. Tearing himself away from yet another computer game, he shook his head—he hadn't heard of the breach, or even of the Skripal poisoning investigation. Just a couple of days later, Russian media reported that the FSB had arrested a border service officer who had allegedly sold internal law enforcement data to Bellingcat and *The Insider*. I was surprised by the story—I had always dealt with middlemen like Vasily, who collect leaks after the fact, not with people who have direct access to the systems themselves. And so, after years of working with the databases, I found myself—for the first time—wondering who was actually leaking them, and why. I began digging through court rulings under criminal code articles on violations of privacy. In Russia, some judicial decisions are publicly available, even if anonymised. In one of them, I stumbled across a reference to an internet forum called *Probiv*.

The court document concerned an employee of the Sberbank contact centre in Voronezh, a regional city south of Moscow. He had posted an advert on *Probiv*, offering—for a fee—to supply information about bank clients. It wasn't just account statements on offer, but even the secret code word that customers set up for emergency access to their funds. He traded the information anonymously—until local security officers came across his ad. They carried out a "test purchase" ($230 for an account statement), then checked Sberbank's internal system to see which employee had siphoned off the records of a specific, pre-identified client.

When I typed the *Probiv* address into my browser, I landed on a forum that looked like a hobbyist site for dog owners or fishing enthusiasts: themed sections, banner ads, and basic email-based registration. But instead of corgis or types of fishing floats, users here were trading personal data—pulled from the databases of government agencies, law enforcement, banks, and mobile phone providers. And unlike what Vasily had been selling, this was fresh, real-time information.

I also came across an ad on *Probiv* offering extracts from the same Rospasport system. At the time, I was working for the BBC Russian Service, which allowed me to carry out a "test purchase" as part of a journalistic experiment: I bought information about myself for $30. A day later, I received a file containing details of all previously issued internal and international passports—complete with photos and scanned copies of the original applications. Among them was the very first form I had filled out back in late 1997, at the age of fourteen. The photo showed the same boy who once dreamed of being a detective and had dropped the agency "Detective" business cards into his neighbours' mailboxes. The billing records for my grandmother's mobile number—showing who she had called and where she had been at the time—cost the newsroom several times more. And even then, we got lucky with the provider: buying similar data tied to my own number from a different operator would've cost around a thousand dollars.

Before publishing my piece about the data "punching" market, I asked Bellingcat whether they had purchased information about the Skripal poisoners. At the time, they told me that an anonymous source had provided them with extracts from Rospasport. But a year later, at the end of 2020, when the same team was investigating the poisoning of Alexei Navalny, Bellingcat not only acknowledged that they had bought data from *Probiv*—they even published

an explanation of what that market was. “We’ve always explained in detail how we arrived at our conclusions,” a former member of the project told me. “In the Skripal case, *Probiv* wasn’t our only source, so we didn’t mention it. But in the Navalny investigation, almost everything came from there—that’s why we decided to spell it out.”

For those who wanted to dig deeper, there was a link to my earlier article—the same one in which Bellingcat had denied everything. The man footing the bill for those expensive editorial requests was Bulgarian journalist Christo Grozev, and the Navalny poisoning investigation would go on to become perhaps the most defining chapter in his unusual career. Just a month earlier, my own major piece had come out—the investigation into Svetlana Krivonogikh and her secret daughter fathered by Putin—while around the same time, the outlet *Vazhnye istorii* published revelations about the private life of the president’s official daughter. It was such a banner year for exposés about Putin that even the president himself had to respond to them at his year-end press conference. That said, the question—posed by a journalist from a pro-Kremlin outlet—couldn’t have been more delicately worded. All the articles were lumped together into a single, soft-touch query: “Some time ago, a number of interesting investigations came out—for example, about your daughter, your former son-in-law <…> and others said to be close to you. And this week there was one about Alexei Navalny.”

“This isn’t some kind of investigation—this is just laundering material from American intelligence services… These guys from the agencies were simply carrying out their orders,” Putin declared[12]. I’d grown used to hearing that kind of accusation from pro-Kremlin propagandists aimed at me. But in Grozev’s case, I noticed something different: the same suspicions would occasionally surface from people who were otherwise staunchly anti-Kremlin. “Is it true that he works for intelligence?”—that was the very first question I got from fellow

[12] Vladimir Putin's annual press conference // http://kremlin.ru/events/president/news/64671

journalists when they found out that, while working on this book, I'd decided to trace the biography of the man behind the most explosive investigative scoops in Russia in recent years.

Chapter 2: A Nerd with a Laptop

At the start of 2018, Bulgarian journalist Christo Grozev was dashing around the Austrian ski resort of Flachau, trying to find a Western Union office — one of the world's largest cross-border money transfer networks. His plan for the day had been simple: relax and go skiing with his kids. But just as he reached the top of the slope, he got a message from a Russian private detective he'd been messaging the night before. The detective wrote that, for $40, he could run a check on the person Grozev was interested in — across the databases of all Russian mobile operators.

That winter, Grozev was working with Bellingcat on the investigation into the downing of Malaysia Airlines Flight MH17 — a Boeing 777 shot out of the sky over eastern Ukraine. The plane, en route from the Netherlands to Malaysia, was destroyed in July 2014 over the Donbas region, at the height of the war there. Using open-source data, Bellingcat quickly determined that the aircraft had been brought down by pro-Russian separatists using a Buk surface-to-air missile system that had been transported in from Russian territory. Investigators traced the launcher's route from the Russian border into Ukraine using videos posted on social media. The key question that remained was: who on the Russian side had coordinated the Buk's deployment to the front?

The investigation was built on recordings of dozens of phone calls made by pro-Russian separatists during the spring and fall of 2014. The wiretaps had been released by Ukraine's counterintelligence agency, the SBU (Security Service of Ukraine). One figure stood out among the separatists' contacts — a man who went by the call sign "Orion." According to the SBU, this alias belonged to a high-ranking officer in Russia's GRU military intelligence. The international investigative team handling the MH17 case issued a public appeal, asking potential witnesses to

help identify the man behind the name. Bellingcat and Grozev had obtained several Russian phone numbers that might be linked to "Orion." But the leaked databases they had access to weren't sufficient to trace or verify the numbers.

While on holiday with his children at the ski resort, Christo came across the website of a Russian private detective agency — its name included the numbers 007 — and sent a message to the contact listed. In his request, Grozev asked the agency to identify the owner of a phone number. The self-styled Russian James Bond replied, suggesting they check the number through the *Probiv* market. "That was the first time I ever heard the word 'probiv'," Grozev recalls. Leaving his kids to ski on their own, the Bulgarian raced downhill to find a Western Union and wire money to Russia — eager to get the request "into the system."

The investigation into "Orion" was published in May 2018.[13] The information Grozev had purchased via *Probiv* revealed that the man behind the call sign was none other than GRU General Oleg Ivannikov. Grozev and Bellingcat held a press conference to present their findings. At one point, Grozev considered showing up in a hat and fake moustache — but in the end, he settled for a pseudonym: *Moritz Rakushitsky*, a made-up surname inspired by the English phrase *raccoon shit*.[14] He even gave interviews under that alias. But before long, it was pointless to hide: the once-unknown 50-year-old Bulgarian had begun releasing one explosive investigation after another. Five years later, he stood onstage at a theatre in Los Angeles — as Hollywood's finest, seated in the audience, gave him a standing ovation.

[13] A Woman's Voice Gave Him Away: GRU General Identified as Key Figure in MH17 Downing // https://theins.ru/politika/103853

[14] Bellingcat Press Conference Concerning Their Investigation Into Malaysian Airlines MH17 Downing // https://www.gettyimages.fi/detail/uutiskuva/moritz-rakuszitzky-and-eliot-higgins-from-the-citizen-uutiskuva/962343096

The Struggle for Long Hair

Resisting the state was a trait that ran in the Grozev family — and their state gave them no shortage of reasons. After the Second World War, Bulgaria fell within the Soviet Union's sphere of influence. A Soviet-style regime took hold: complete with its own Communist Party, homegrown strongmen, and, like the rest of the Eastern Bloc, an "Iron Curtain" sealing it off from the West. Even the country's official name underscored the regime's character — not just a republic, but the People's Republic of Bulgaria (PRB).

His father, Grozyu Grozev, worked as a math teacher in a small town near Plovdiv and eventually rose to the position of headmaster. But then he was faced with a stark choice: either cut his long hair or resign. The elder Grozev, ever the rebel, chose to keep his hair — and with his dismissal came a *"wolf ticket"*, an unofficial blacklisting that made it nearly impossible to find work as a teacher in Soviet Bulgaria. At the time, the ruling Communist Party saw a hippie hairstyle as a symbol of political unreliability and "servile admiration for the bourgeois West." People like that, the authorities believed, had no business educating children in a socialist state.

Grozev Sr. found work as an elevator repairman in Plovdiv and moonlighted as a tailor in his spare time. Expelled from the education system by an authoritarian regime, he sometimes used authoritarian methods of his own when raising his son. A staunch Americanophile, he insisted that Christo study English instead of French, and later — against the boy's wishes — enrolled him in the English-language high school in Plovdiv. With that kind of linguistic training, the natural next step would have been to study philology at Plovdiv University. But Grozev Jr. was only interested in two things.

The first was journalism. As a teenager, Grozev wrote for the Komsomol press in Plovdiv, trying — as he later put it — to sneak a bit of "dissent" into the pages of an otherwise censored publication. His second passion was closely tied to the first. When Christo was around ten, his father brought back a pair of rudimentary walkie-talkies from the Soviet Union. The future investigator of Russian security services turned them into a makeshift home radio station, broadcasting news to his grandparents — who lived in the same house, just one floor down. As he got older, he would spend hours tuning in to foreign music stations, dreaming of one day launching an independent station of his own.

Thanks to his studies in English, Christo Grozev was selected for a group of Bulgarian students sent to London for professional experience. It was the summer of 1989. Perestroika was in full swing in the Soviet Union, and its ripple effects were beginning to shake the foundations of the Eastern Bloc's "people's democracies." While in the British capital, Grozev gave an interview to Radio Liberty — a station originally created by the CIA to broadcast into the Soviet sphere. "How does it feel," the host asked, "to know that your entire life will be lived under communism?" "You don't understand," Grozev shot back. "Communism is going to fall — and soon." In Bulgaria, his prediction came true just a few months later. But that brief window was enough: Grozev was expelled from university in a political scandal.

Along with the collapse of the pro-Soviet regimes in Eastern Europe, the Iron Curtain came down too: Bulgarians could now travel abroad freely — if they could afford it. By that time, Christo's father had already left his job as an elevator repairman. During the years of Soviet-era shortages, his garage hobby of sewing made-to-measure clothing had quietly grown into a real business. And as soon as the People's Republic of Bulgaria (NRB) legalized private enterprise, Grozev Sr. officially registered as an entrepreneur. "My father stood in line outside

the courthouse all night so his company could be the first one registered," Christo recalls. As for Christo himself, after being expelled from university, he decided to take full advantage of the newly open borders. He applied to a university in the Belgian city of Liège, where he had independently found a tuition-free program for Bulgarian students.

He was accepted, and in the summer of 1990 Grozev arrived in Belgium to look for housing and get ready for the start of the academic year. But first, he decided to hitchhike to nearby Luxembourg — home to the famous Radio Luxembourg. Thanks to its powerful transmitter, the station had spent decades delivering the latest music — no boring news, no politics — to young listeners on both sides of the Berlin Wall. Christo had been one of its devoted fans. "I used to call them all the time from Bulgaria and win all sorts of contests," he recalls. Now, he was ready to meet them in person.

The DJs at Radio Luxembourg welcomed the Bulgarian teenager warmly and offered Christo an internship. He gladly accepted and rented a small room from one of the station's staff members. Each day, on his way to the studio, he passed the embassy of the fading People's Republic of Bulgaria. The modest two-storey building looked deserted: no one came in, no one went out. One day, curiosity got the better of him — he peered through a window. No staff were in sight. Papers lay strewn across the floor, as if the building had been vacated in a hurry. Unable to resist, Grozev climbed through the window and began rummaging through folders marked *"Secret."* The aspiring journalist realised he'd stumbled upon a goldmine. He spent the next two weeks poring over the discarded documents of a vanishing regime.

Around the same time, citizens of the German Democratic Republic (GDR) were combing through similar folders. After the fall of the Berlin Wall in the autumn of 1989, they stormed local offices of the Stasi, East Germany's secret police — partly to prevent agents from

destroying records of surveillance against ordinary citizens. In the Luxembourg embassy of the People's Republic of Bulgaria, Grozev discovered internal denunciations: employees writing each other up for ideological misconduct. One report noted that “Comrade So-and-so, instead of marking an important Communist holiday, went out drinking with Russian émigrés.” Other documents revealed that the NRB had been financially supporting the Communist Party of Luxembourg — apparently clinging to the utopian belief that even this wealthy Western state might one day see a proletarian revolution.

The former Komsomol newspaper contributor from Plovdiv dreamed of writing an exposé about Bulgaria’s ruling elite — all of them products of the Communist Party of the People’s Republic. He planned to base it on the sensitive archival material he had uncovered. But just two weeks after slipping into the embassy building, Grozev was detained by Luxembourg authorities, who confiscated his notebook filled with handwritten excerpts. So, his investigative ambitions had to be put on hold. Grozev wouldn’t return to that genre for another twenty years.

After being interrogated on suspicion of espionage, Grozev was expelled from Luxembourg. He never returned to Belgium to resume his studies — after his time at Radio Luxembourg, he had a new goal in mind: launching a station of his own back home in Bulgaria.

Radio "Aura"

In 1991, the Open Society Foundation — founded by philanthropist and entrepreneur George Soros — opened a university in the Bulgarian town of Blagoevgrad. Grozev Sr., a devoted Americanophile, bundled his son into their brand-new Lada Samara and set off for the other side of the country. Plovdiv, their hometown, sits in the south; Blagoevgrad lies to the southwest, near the borders with Greece and North Macedonia. The drive between the two takes about half a day

— a considerable distance by Bulgarian standards. “Blagoevgrad felt so far away,” Christo recalls. “I told my father there was no way I could live there for four whole years. But he just slammed the car door — and off we went.”

Ironically, I’m speaking to him over the secure messaging app Signal while sitting in Blagoevgrad myself — my wife, a Bulgarian, happens to be from here. The university’s campus still stretches along the banks of the Bystritsa River, nestled in the mountains. It’s a peaceful, almost idyllic spot — no wonder one of the buildings once served as the residence of Todor Zhivkov, the longtime leader of socialist Bulgaria.

In Blagoevgrad, Grozev teamed up with fellow students to fulfil a long-held dream: they launched a local station called Aura, which went on to become the first private radio station in Bulgaria. They broadcast a mix of rock, pop, and news — a radical departure in 1991, when most state-run stations still clung to stiff, Soviet-style programming. At first, the studio’s soundproofing was cobbled together from apple shipping crates, and Christo sourced second-hand equipment from the Netherlands for $350. The gear had once belonged to a pirate radio station that broadcast into Europe from a ship at sea. There’s a photo of young Christo on the university’s website. He hasn’t changed much over the years, apart from his noticeably thinning hair. His eyes are sharp and intelligent, and there’s a familiar mix of fatigue and vulnerability in his expression — the kind that immediately makes people trust him.

The success of Radio Aura caught the attention of managers at the American media company Metromedia, which had begun expanding into post-Soviet countries in the early 1990s. Grozev hadn’t even graduated yet, but he already had a promising job offer: the Americans asked him to go to the Russian city of Sochi to help set up a network of commercial radio stations there. Like all Bulgarians during the socialist era, Grozev had studied Russian in school — but

before setting off, he decided to test himself. In Blagoevgrad, he found a Russian woman and invited her to lunch. After enduring a meal peppered with Christo's confused use of grammatical cases, she smiled and delivered her verdict: "Well, what can I say — you're lucky Sochi doesn't decline." Today, after years of living in Russia, Grozev hardly makes mistakes at all. In fact, he occasionally uses Russian words in place of Bulgarian — for instance, saying *razvedka* (intelligence) instead of *razuznavane*.

Grozev arrived in Sochi — the resort city on the Black Sea — in the summer of 1995. There, he quickly got Radio Nika off the ground, a station that mixed trendy music with news and entertainment shows. The project turned a profit, and the pleased executives at Metromedia soon asked him to head to St. Petersburg to help strengthen their team there. At the time, all foreign business in the city was overseen by Vice-Mayor Vladimir Putin. Grozev doesn't recall ever meeting him directly, but he's confident their paths must have crossed — Putin's signature appears on the permits and paperwork that authorized his stations to operate in the city.

In 2000, former vice-mayor Vladimir Putin became president — and the American media holding Metromedia began running into trouble in Russia. First, people connected to billionaire Vladimir Yevtushenkov's conglomerate Sistema infiltrated Metromedia's Russian operations through a convoluted scheme. Grozev describes the episode bluntly as a "raider takeover." [15] For a time, the Russian branches of Metromedia were formally registered under Grozev's own name — partly, he says, to shield them from censorship. But by the mid-2000s, both the Americans and Grozev had fully divested from the ownership of all the radio stations. The new owner soon gave journalists a clear directive: "Don't hit Putin. He's one of ours."[16]

---

[15] President of Metromedia International Group Inc., Mark Hauf // https://www.comnews.ru/content/49969; Yankees Go Home: Metromedia and 'Indigo' Leave Russia // https://www.comnews.ru/content/2188

[16] A Frenchman Boards Russian FM Radio Stations // https://www.inopressa.ru/article/13Mar2006/liberation/fm.html

Grozev didn't hold a grudge against Russia, even after spending more than a decade there. "Of course, I was troubled by what was happening," he says of the fate of the media projects he had built. "Right after the sale, the newsroom was told: 'No negative news.'" But his passion for the media business didn't fade. He settled in Vienna and invested in launching a music radio station in the Netherlands — and later, another. His partner in the venture was Carl von Habsburg, grandson of the last emperor of Austria-Hungary. The Habsburgs had once ruled one of Europe's great empires, until they lost power and property in the 1918 revolution. For conspiracy theorists who believe Grozev is backed by powerful forces, this connection is irresistible. They like to cite the Habsburg name, claiming that the family are key players in a secretive global elite that pulls the world's strings.[17] Grozev brushes off such talk. He says he met Carl von Habsburg at a management course in Italy in the early 2000s, and their shared classes turned into a friendship. "He has neither influence nor money," Grozev says, laughing off the mythology surrounding his friend.

In the late 2010s, Grozev and his partners decided to expand their media investments beyond the Netherlands and turned their sights to his native Bulgaria. By then, the Balkan country had joined the European Union, and Grozev hardly expected to encounter even fiercer resistance from figures close to the state than he had in Russia. Their attempts to acquire Bulgarian media — first a cable TV channel, then several popular daily newspapers — ran into a brick wall: Delyan Peevski, a powerful media baron often described as the "grey cardinal" of Bulgarian politics. Grozev filed complaints against Peevski and his associates with the European Commission, launched lawsuits in Sofia, and gave frequent interviews to the Bulgarian press. But in the end, he and von Habsburg were left with nothing. In one particularly theatrical twist,

[17] How the Spy Case Against Christo Grozev Is Being Whipped Up in Bulgaria // https://dzen.ru/a/Y6wiiqq_PRqabSj_

they suddenly discovered that their majority stake in the newspapers had been quietly transferred to other individuals — reportedly linked to Peevski.[18] Meanwhile, Grozev's business rivals claimed he was the one cutting backroom deals with the media tycoon.[19]

"They kicked me out of Russia politely — at least they paid me. But here, they just stole the money. It's a disgusting story, and it sparked in me a real urge to fight. Adrenaline — so much adrenaline," Grozev recalls. He began digging into how Peevski was tightening his grip on the media — and whose money was behind it. The trail led to the Cooperative Trade Bank, where many Bulgarian state-owned companies kept their funds. That money, it turned out, was used to buy up media outlets — the same ones where the bank, along with state-affiliated companies, then placed their ads.

Grozev didn't publish his findings — instead, he submitted them to the European Commission as evidence of legal violations. It didn't help in his battle with Peevski (who would only fall under U.S. sanctions for corruption in 2021), but it led to an important personal realisation. "I understood that, even as a private citizen, I could carry out a full-fledged investigation capable of persuading a government body," he says. That was how Grozev returned to the path once cut short by Luxembourg's security services, who had confiscated his notebook all those years ago. The pivot may have seemed sudden — even suspicious: a successful media executive abruptly trading boardrooms for fieldwork, chasing leads and writing stories again. But that's exactly what he did — stepping straight into the thick of investigative journalism.

---

[18] Съдът махна Христо Грозев от «Труд» и «24 часа» // https://www.mediapool.bg/sadat-mahna-hristo-grozev-ot-trud-i-24-chasa-news195537.html; Скандалът за «24 часа» и «Труд» премина в истерия // https://frognews.bg/novini/skandalat-24-chasa-trud-premina-isteriia.html

[19] Съдружниците в «Труд» и «24 часа» с взаимни обвинения за «мръсни пари» // http://web.archive.org/web/20140314175038/https://www.mediapool.bg/sadruzhnitsite-v-trud-i-24-chasa-s-vzaimni-obvineniya-za-mrasni-pari-news185530.html

"Even as a teenager, I loved telling people things they didn't know — my parents, friends, whoever," is how Grozev explains his motivation.

His friends, too, find nothing unusual in how things turned out. "He was always incredibly observant, like Sherlock Holmes. Once, he overheard a conversation at the airport and ended up using that information in business. So no, I wasn't surprised — he's simply found his calling in investigations," says a family acquaintance.

By 2014, Grozev had already stepped back from actively managing his media assets in the Netherlands — they were bringing in a steady income on their own. That freed up time for him to return to journalism, and Russia's newly launched hybrid war against Ukraine gave him no shortage of reasons to investigate.

The Case of the Codpiece

At first, investigative journalism was just a hobby for Christo: in the mid-2010s, he even officially referred to himself as a *hobby researcher*. Around 2013–2014, Grozev began collaborating with a research centre at the private New Bulgarian University. The centre was headed by former Bulgarian Prime Minister Ivan Kostov, known during his time in office for supporting European integration over alignment with Russia. Even the centre's logo resembled that of NATO. In March 2014, for example, Grozev gave a talk there on how Russian propaganda was portraying events in Ukraine — from the annexation of Crimea to the Kremlin-backed protests in the country's southeast.[20]

[20] Електронатa война срещу Украина // https://eprints.nbu.bg/id/eprint/2742/1/%D0%94%D0%A0%D0%A1%20%D0%90%D0%A1%20%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%82%D0%B0%20%D0%B2%D0%BE%D0%B9%D0%BD%D0%B0%20%D1%81%D1%80%D0%B5%D1%89%D1%83%20%D0%A3%D0%BA%D1%80%D0%B0%D0%B9%D0%BD%D0%B0%2C%20%D0%A5%D1%80%D0%B8%D1%81%D1%82%D0%BE%20%D0%93%D1%80%D0%BE%D0%B7%D0%B5%D0%B2.pdf

Christo also tackled Kremlin propaganda and its fakes on his blog, hosted on the publicly available WordPress platform. At the time, he was not yet familiar with leaked databases — let alone with the black market world of *probiv*. Writing about yet another Russian activist who had travelled to fight alongside the separatists, Christo would candidly admit that he had no way of knowing whether the man was an FSB agent or not.[21] A few years later, he would have the tools to find more definitive answers to questions like that.

At some point, Grozev was contacted by Eliot Higgins — a Briton who, like him, had started doing investigations as a hobby (Higgins was a financial analyst by profession) before turning it into a full-time job. In 2013, using only open-source data, Higgins proved that the Syrian government had used chemical weapons against rebel forces. The following year, he launched a crowdfunding campaign, built a team, and founded the investigative outlet Bellingcat. Just two days after its launch, a Boeing airliner was shot down over Donbas, and Higgins' Twitter followers urged him to investigate the incident. Grozev, who was also sharing links to his findings on Twitter, caught his attention — and it was only natural that Higgins invited him to join forces. Grozev's wife encouraged him to accept: "You're doing investigations anyway — at least this way you'll have some kind of backing," recalls a family friend.

"That was Bellingcat's golden age," Grozev recalls nostalgically. "Eliot immediately added me to a Slack chat where I could see what investigations were in progress. It was all very informal — full of energy, enthusiasm, and a real sense of camaraderie. You just had to be ready for the collective nature of the work, for colleagues to question you and ask, 'Where did you get that fact?' or 'What's your source on this?'"

Bellingcat's partner in Russia became the up-and-coming outlet The Insider, founded by former political activist Roman Dobrokhotov. Grozev and Dobrokhotov connected over a shared

[21] Russia's deniable war // https://cgrozev.wordpress.com/author/christogrozev/page/8/

interest in Konstantin Malofeev — a Russian Orthodox businessman and one of the key sponsors of Russia's hybrid war against Ukraine in 2014. Grozev frequently posted about Malofeev on Twitter, and Dobrokhotov eventually reached out to him — much like Higgins had done before. That marked the beginning of their first joint investigation, *The Kremlin's Octopus*, which examined Malofeev's activities in the Balkans.

Through Dobrokhotov, Christo gained access to leaked databases from Moscow radio markets. But leaks had their limits — for instance, they couldn't confirm the current owner of the phone number linked to "Orion," the figure from the intercepted calls between pro-Russian separatists in Donbas recorded by Ukraine's SBU. Looking for more up-to-date data, Grozev turned to the website of a Russian detective agency with "007" in its name and, while vacationing with his children at a ski resort in early 2018, made his first purchases on *probiv*. For that case — and all those that followed — Grozev says he paid out of his own pocket. Bellingcat's core funding comes from NGOs to support open-source training, and using that money for *probiv* would have been ethically out of bounds.

After *Orion*, Grozev and Dobrokhotov began turning out one bombshell investigation after another—still without drawing too much attention to the fact that they were buying personal data on their subjects. Using information from the *Rospasport* system, they demonstrated that the poisoning of ex-GRU officer Sergei Skripal and his daughter in Salisbury, England, had been carried out by GRU operatives Mishkin and Chepiga (2018). They identified the agents who tried to poison Bulgarian arms dealer Emilian Gebrev—also GRU officers—by using travel records from the police database *Rozysk-Magistral*, which tracks all domestic and international trips taken by Russian citizens by plane or train (2019).[22] Billing records from mobile operators,

[22] The Poisonous Eight: How and Why 8 GRU Officers Tried to Poison Bulgarian Businessman Gebrev with Novichok // https://theins.ru/politika/189327

bought via *probiv*, allowed them to name those inside Russia responsible for manufacturing the lethal Novichok nerve agent used to hunt down enemies abroad (2020). And then came the pinnacle: the investigation into how FSB operatives attempted to poison Russian opposition leader Alexei Navalny—built on data from every available source: *Rospasport*, Rozysk-Magistral, and mobile phone providers.[23]

Calling it "the pinnacle" is my own subjective assessment of the work done by Bellingcat and The Insider. Sitting in Vienna and buying data through *probiv*, Grozev was able to uncover what had happened on the other side of the continent—in Western Siberia, in Tomsk—where, on 19 August 2020, security agents apparently broke into Alexei Navalny's hotel room and laced his underwear with the nerve agent Novichok. Data from the *Rozysk-Magistral* system confirmed suspicions that the same FSB operatives had been tailing Navalny for years, traveling to the same cities he visited. Billing records—which reveal a phone's location at the time of calls—showed that on 19–20 August, they were in Tomsk, including near his hotel. The same records showed the poisoning team maintained regular contact with chemical weapons specialists at secret Russian research institutes. Finally, entries from the *Rospasport* database revealed that they used fake identities when traveling.

The investigation was captured on camera by American documentary filmmaker Daniel Roher, who was then working on a film about Alexei Navalny. It gave rise to one of the most iconic—and entirely genuine—scenes illustrating how modern investigations unfold. At one point, Navalny's team, together with Grozev, decided to try a bold move: they would cold-call the FSB officers involved in the poisoning, posing as an aide to the Secretary of the Security Council, in hopes of confirming their complicity. Most of the men hung up almost immediately.

[23] The Case Is Solved: I Know Who Tried to Kill Me // https://navalny.com/p/6446/

But then Navalny dialed the number of military chemist Konstantin Kudryavtsev—and, to everyone's astonishment, Kudryavtsev began speaking to him as if he were a colleague.

"Who gave the order to treat the crotch area of the underwear?" Navalny asked, his voice serious.

"They said to work on the underwear, on the inside part," Kudryavtsev replied.

At that moment, Christo Grozev appeared on camera too: sitting beside Navalny, he buried his face in his hands, struggling to suppress laughter—unable to believe that an FSB officer had actually fallen for a simple phone prank and unwittingly confirmed all the suspicions he and his colleagues had formed based on data from the *probiv* market. Still, Grozev had suspected that Kudryavtsev might be the one to take the bait: it was early morning when Navalny called—deliberately timed to catch him off guard. The caller ID had been spoofed to show the FSB's switchboard number, and they reasoned that a scientist from a defense research institute might not be as versed in counterintelligence tactics as a career security officer.

After the release of both the investigative reports and the documentary *Navalny*, Christo Grozev became a global star of investigative journalism, giving interview after interview and openly discussing the *probiv* market. Eventually, his name was heard from the world's biggest stage. "We're very grateful to our laptop nerd, Christo Grozev," said director Daniel Roher, accepting the Oscar for Best Documentary in March 2023, as he pointed the statuette toward the tuxedoed investigator standing behind him. "Christo, you risked everything to tell this story."

By this time, the risks were no longer theoretical but very real — and far more serious than that run-in with the Luxembourg police.

"Agent Christo"

On 15 December 2021, the day after the Navalny poisoning investigation was released, former Austrian counterintelligence officer Martin Weiss contacted his former subordinate, Egisto Ott, asking him to look into Grozev, who was living in Vienna. Ott obtained Grozev's address from the local equivalent of a civil registry office, then drove to the journalist's house and took photos of it. Both Weiss and Ott, now working for financier Jan Marsalek, continued to leverage their connections within Austria's main intelligence agency. Grozev would later discover that Marsalek maintained close ties with Russian security services. [24]

A source in Western intelligence warned Grozev in time about the threat from the Russian security services. He was forced to leave his beloved Vienna after twenty years of living there and has since kept his permanent location secret, seeing his family only occasionally. His father passed away in 2023, having spent his final years in Austria; despite this personal tragedy, the local police allowed Christo to see his relatives only in a safe house, and only for two hours. If an old acquaintance he hasn't spoken to in years suddenly reaches out suggesting a meeting, Grozev declines: he can't know what's behind the gesture—genuine affection or Russian intelligence money. He knows that Marsalek, in his hunt for him, hired several Bulgarian nationals, and they discussed whether it might be possible to kidnap Christo and smuggle him into Russia. [25]

He cannot return to his native Bulgaria even for a couple of days—he has noticed surveillance there, and the country is generally considered unsafe due to the potentially high presence of Russian agents. In Russia, where Grozev lived for nearly a decade, he became the target of several politically motivated criminal cases following the start of the war in Ukraine and

[24] "From conman to priest. How the security services are hiding Jan Marsalek in Russia, who stole billions of dollars. // https://theins.ru/politika/269604

[25] Man who spied for Russia in UK "discussed killing journalist"// https://www.bbc.com/news/articles/c20gvl0x8yyo

was declared wanted in absentia. The last time he visited Moscow was in 2016 to lead a seminar for radio journalists; upon leaving the country, his visa was revoked—a clear signal from the Russian security services about how they viewed his work.

The criminal prosecution has, of course, been accompanied by a barrage of public accusations. On Russian state television, Grozev is officially labelled an "agent of British intelligence," while *Tsargrad*—the outlet run by Konstantin Malofeev, the subject of several of Grozev's investigations—refers to him as an agent of "American intelligence services." Some of Grozev's discoveries truly do defy explanation through *probiv* alone. For example, in the investigation into the poisoning of Bulgarian arms dealer Emilian Gebrev, Bellingcat used photographs of GRU officers taken from Schengen visa applications—material that is obviously not available through *Probiv*, which only includes data from Russian government agencies and companies. A 2024 report on Jan Marsalek also included information drawn from a criminal case against the international fraudster and his Austrian accomplices.

"In recent years—and especially after the Oscars—law enforcement has increasingly come to me for help. I won't deny that I've assisted them," Christo admits in our conversation. "But it's always the police and other law enforcement agencies, not intelligence services." He's quick to add, however, that almost none of them ever provide him with information—"they only take." Still, based on the kinds of questions they ask (say, "Did such-and-such person arrive in Vienna?"), Grozev can infer what they already know—and begin digging from there himself.

"Don't you ever regret becoming an investigative journalist—someone now hunted across the globe by vengeful Russian security services?" I ask Christo. "I can't imagine another life that would excite me this much. I've never been as happy as I am now. So no—no regrets," he replies without a moment's pause. Nor does he regret spending a quarter of a million dollars

of his own savings on *probiv*. "And what does your wife think about spending the family savings that way?" I ask.

"All the worst," he says with a wry smile.

Grozev's investigations have radically and irreversibly changed not only his own life—they often end up shaping the fate of those who deal with him on the *probiv* market as well: the FSB starts hunting them down. "I don't lose sleep over the police officers selling that data," Grozev says of his approach. "They're not just helping me—they're helping killers and thieves too. So I don't feel any guilt if they get arrested. But the fate of the middleman—that's a different story."

One such intermediary was a young man from the Russian provinces named Alexei. He got into the *probiv* business for the money, sold Grozev a significant portion of the data related to Navalny's poisoning, endured pressure from the security services, and—thanks to Grozev—managed to flee Russia with his family before he could be arrested.

Chapter 3: A Man from the Middle of Nowhere

When Christo Grozev and his colleagues published their investigation into the poisoning of Alexei Navalny in December 2020, it was discussed not only by politicians, journalists, and opposition-minded citizens. Russian *probivshchiki*—data brokers operating on the black market—also took notice, though they were interested in rather different questions than the average reader.

Here's one of their exchanges from a private Telegram chat:

"I wrote that RPs (extracts from the *Rospasport* system—Author's note) are 600 [rubles, which is around 7 dollars] now?"

"No. Well, okay. No problem."

"Things are tough right now. The only option left is a pricier one. Thanks, Navalny."

The difficulties arose because, after the investigation was published, police officers who had been selling information from the Interior Ministry's internal databases temporarily stopped working with the data brokers.

"That Navalny really stirred some shit up. Total fucking mess."

"Big time. Now even more people want to take him out."

The main question was who had sold Christo Grozev and his team the data on the poisoners. "Was it your guy who sold the info on those feds?" one data broker asked another.

The participants in these chats knew each other only by their Telegram handles—names like Mr. Leo, Nsolo, or Soulful Bidzho. But two of them, PDE and Redadmin, were friends who also kept in touch outside the messenger. They too ran checks on the names of the FSB officers who had tried to poison Navalny, using their own sources—but at first, they came up empty.

"Then they double-checked and realised it was us who'd sold the info," Redadmin tells me, sitting on a park bench somewhere in Europe. Back then, in late 2020, he was living in a small Russian town, feeling a mix of pride and fear. As it would soon turn out, the fear was more than justified: just a few months later, he would end up in the back of a minivan, his head wrapped in duct tape and a raw potato stuffed in his mouth.

"Bro, what've we got for Monday?"

By the time he was 25, Alexei[26] had already served in the army, worked on a construction site in Moscow, wrecked his back there, and returned to his hometown—a satellite town near a regional centre on the banks of the Volga. Jobs were scarce, and the going wage (up to 30,000 rubles, or around $450) held no appeal for him. "I didn't want to work for that kind of money. I tried driving a cab for a while, but I hated having strangers in my car," he recalls. He and an old acquaintance, Alexander, opened a small shop selling phone accessories, but they picked a bad spot, and the place didn't last three months. It turned out, though, that Alexander—a chubby guy with glasses—had another side hustle going. He offered his drifting friend a stake in it. Though really, his *business* probably deserves quotation marks.

For several years, Alexander had been working as a data broker—taking requests from clients who wanted access to information from police, tax, or mobile operator databases, and forwarding those requests to specific insiders within those agencies. Both sides knew him only as an anonymous figure on Telegram, under the handle PDE. In this world, a nickname functions like a brand: clients stick with the info dealers they trust and switching accounts can mean losing your regulars. Alexander also had another well-established account—Redadmin—but he didn't

[26] Names, messenger nicknames, and certain personal details have been changed at the request of the individuals in this chapter, for security reasons.

have the time to keep it going. So he offered it to Alexei, suggesting he take it over and develop it himself.

All the data brokers whose stories I know were drawn to the trade by a mix of things: a desire to live well, curiosity about internet-based businesses, and a lack of decent, legal ways to make money in their regions (or at least, that's how it seemed to them). One young man from Siberia, who would eventually end up with a criminal record for selling personal data, was enticed by the idea of earning 200,000–300,000 rubles a month—several thousand dollars at the time—and by how easy it was to break into the business. "I was just finishing school, hanging out on forums about making money online—that's where I first heard about *probiv*," he told me. It was there, on those *probiv* forums, that he started looking for police officers willing to sell information. And when it came to finding insiders at mobile operators, he just spammed the same message across public VKontakte groups—ones like "Overheard at Beeline." "A lot of *probivshchiki* (data brokers) with the gift of gab just walked into phone shops and pitched the job straight to employees," he recalls.

Alexander—aka PDE—was working at a mobile phone shop when he first heard about the data-leak business from a friend in another city. They used to team up to grind in the online shooter Counter-Strike. The friend was already making money on the market, and the way he described it sounded so enticing that Alexander quickly got involved himself. Before long, he was pulling in more than 200,000 rubles a month—a huge sum for a Russian provincial town in the late 2010s. So when he offered Alexei a piece of the action, there wasn't much hesitation.

"We knew it was illegal, that it could end with us in prison. But I saw how many people were selling data—and nobody gave a shit, nothing was happening to them," he says years later. Alexei is a modest, soft-spoken guy with a round, gentle face and a quiet laugh—like he's afraid

that laughing too loudly might make you uncomfortable. He doesn't look anything like someone who once sold other people's personal data to just about anyone—including fraudsters. "Of course I thought about the harm I might be causing," he goes on. "But I also understood that if I got out of the game, whoever was looking for those leaks would just buy them from someone else anyway."

At the time—as now—the cheapest data came from government databases. In 2020, an extract from the *Rospasport* system cost from 1,000 rubles (about $14); a report from the *Rozysk-Magistral* system, listing all of a person's train and air travel, started at 1,500 rubles ($20); and access to the traffic police database, with full vehicle information, could be had for as little as 500 rubles ($7). Extracts from the Pension Fund or tax office showing all places of employment and income totals ran to a few thousand rubles. Mobile data was more expensive, and prices varied depending on the operator. For instance, identifying the owner of a Beeline number cost around 400 rubles ($6), while getting a full month's call records—including timestamps and recipient numbers—started at 2,500 rubles ($35). Accessing databases of other telecom companies cost more, especially if the request included the user's location at the time of a call. Finally, tracking bank account activity at major institutions—including the state-owned giant Sberbank—cost on average 10,000 to 20,000 rubles ($150–300). These prices were for end clients: the fee would then be split between the middleman (the "data broker") and the insider—an employee of a government agency, mobile provider, or bank.

Alexander and Alexei promoted their services on underground forums—I found the URL of one such site in a court ruling against a data dealer while working on a BBC article about this market. These forums offered much more than just personal data: you could order fake documents, commission an email hack, launder money, or even choose a stolen car. It was also

through these same forums that employees of state and private institutions—people with direct access to internal databases—would approach data brokers via private messages. "Good afternoon! I work for the FSIN (Federal Penitentiary Service; responsible for prisons – Ed.). I've got data on inmates and plenty of other information from the colony," read one such offer of cooperation they received in the autumn of 2020.

Their main business asset was a police officer known to them only by his Telegram handle—Park House. But that was all they needed: the two friends were interested in data from the Interior Ministry's internal databases, and Park House delivered it reliably—and, crucially, at rock-bottom prices. Extracts from Rospasport, for instance, went for just 200 rubles apiece—two to three times cheaper than what other cops leaking data to the *probiv* market were charging at the time. The data came in bulk. On a single evening in December 2020, Park House sent about ten Rospasport reports to the data broker Denis, including one on well-known Russian feminist Nika Vodwood. (She had been denounced that year for "LGBT propaganda"—possibly prompting the informant or pro-government journalists to dig up more on her.) "Bro, what do we have for Monday?" was the kind of message Park House might casually drop to his partners on a Sunday night.

Behind the nickname was Senior Lieutenant Kirill Chuprov of the Samara police. At 28, he hadn't started a family, had no children, and hadn't really found his calling. In early 2020, he was working the front desk at one of Samara's police precincts, then transferred to street patrol duty—only to ask for a transfer back just a few months later. By all appearances, it was a calculated move: to gain access to the Interior Ministry's databases and start selling the information. To make real money, he needed unrestricted access to all internal systems—something only the department head, Major Alexei Borisov, had. Chuprov pitched him

the promise of easy, serious cash. Borisov not only let him use his office computer, but also handed over another officer's login credentials—without that officer's knowledge.

Business was booming: at the end of each shift, Chuprov would stay behind in his boss's office, churning through orders in batches. "Bro, I'm on a call-out [at a crime scene], I'll be back soon and upload everything," he would write when delayed. Word quickly spread among other data brokers about this valuable contact, and they began reaching out to PDE and Redadmin (Alexander and Alexei) to get access to Chuprov. It was fast and cheap—an ideal combo. Brokers often shared their go-to sources with each other. They kept internal Telegram chats where they griped about clients, looked for help with tough orders, or just shot the breeze.

"Anyone need FNS [Federal Tax Service] access? Got a new contact,"—a message like this popped up in one of the chats in December 2019.

"Small stuff? I'll take it," one participant replied, clearly referring to the low purchase price by "small stuff."

"Who's got *Migrant*?" asked Mr Leo, one of the *probivshchiki*. The *Migrant* system of the Ministry of Internal Affairs holds information on all foreigners who enter Russia legally; Mr Leo was looking for data from it.

"Svyaznoy had it. Vilasco too," came the reply, naming the handles of *probivshchiki* who worked with people that had access to that database.

Chuprov made up for the low prices with high volume. Between September and December 2020 alone, he and Borisov earned at least 600,000 rubles by selling data from internal databases. The money was funneled into an e-wallet on the QIWI payment system, registered in the name of one of Chuprov's acquaintances. For a small cut, that same

acquaintance would cash out the earnings and hand them over in person—sometimes behind the police station, by the garages.

The pay boost was significant: at the time, police officers in Samara were earning an average of about 34,000 rubles a month. And both the lieutenant and the major had every reason to expect their earnings to keep rising—because the more media outlets wrote about the data-leak market, the more clients it attracted.

Rules of the Black Data Market

"Data of any complexity cracked," reads a shimmering banner featuring actor Benedict Cumberbatch as Sherlock Holmes. His right eye is mechanical—like the Terminator's in James Cameron's films. This is one of the ads on Russia's oldest underground forum for trading illicit data. The slogan of the anonymous site: "We crack the uncrackable, we talk the untalkable."

Beyond that, everything looks just like a typical forum for dog lovers or fishing enthusiasts: discussion threads, shop pages with customer reviews—only here, what's being sold isn't puppies or bait, but personal data.

"Clear and prompt job on the FTS request." "Asked for a bunch of info—got everything fast, in full, even a little extra. Strongly recommend!" "Everything done cleanly. Quick, no bullshit. Prices were fair."

That's the kind of feedback you'll find on the profile of a seller going by *Leonov Docent*, whose avatar is a character from the Soviet film *Gentlemen of Fortune*. To contact him via Telegram, you have to register—guest users can't see the contact info. The forum itself is easy to find: it shows up on the first page of Google if you search for *information probiv*. There are also dozens of Telegram chats advertising the same services.

There's an unspoken rule in the market: never ask a client why they need the data. Some refuse orders involving children or the elderly, but overall, there are few moral boundaries—for most data sellers, personal information is just another product, no different from a fishing rod. It's widely accepted, both in and around the market, that the main buyers are scammers, private investigators, or corporate security officers collecting intel on suspicious employees or business rivals. Ekaterina Shumyakina, a well-known Russian private detective and former criminal investigations officer, confirmed to me that using the probiv market is standard practice among her peers. "Of course we've used it, and we'll keep using it," said a security officer from a Russian company—one of PDE's clients. The motives can vary: say, a job candidate for a finance department role might need to be checked for prior convictions under economic articles. The easiest way? An extract from the Ministry of Internal Affairs database.

Sometimes ordinary people turn to *probiv* services themselves, bypassing intermediaries like private detectives—say, husbands suspecting their wives of cheating. One *probivshchik* told me about a man who once asked him for his father's credit history. "He said: 'My old man's on a bender—I've no idea where he's getting the money,'" the client explained. The credit report showed that the father had taken out a loan from a microfinance company to buy alcohol. There are also cases where people use *probiv* to search for missing relatives. Police are often reluctant to file a missing person report if too little time has passed—it's more paperwork, and they assume the person might just be drinking or out partying. In situations like that, you can buy what's called a *flash*—data from a mobile operator showing the phone's location at a specific moment. "I remember we talked about one such case in the chat," recalls Alexei, aka Redadmin. "A woman was trying to find her missing teenage son. At first, no one wanted to take the job. Then she wrote: 'Buy my registry office file first (the system for recording births, marriages,

divorces, and deaths—Author's note), just so you know I really am his mother.' They believed her, sold her the *flash*, and I think she found the kid."

Another rule: don't go after high-profile figures. Before accepting a job, both data brokers and their sources typically run a name through Google. The reasoning is simple—public figures, especially those with ties to the state, have the means and the connections to track down and punish not just the leaker but the middleman as well. After all, we're talking about crimes that fall under multiple articles of the criminal code. Caution among data brokers has grown over the years, along with the number of criminal cases involving illegal data sales. Where once a quick glance at the first page of search results was enough, now they may take time to thoroughly vet a potential target. Still, for the right price, they might take the risk: I know for a fact that one broker once sold the recent income history of the famous rock singer Sergei Shnurov—for a price several times above the going rate.

One time, a client came to Redadmin with a request to obtain data on the popular musician Morgenshtern from the *Rospasport* database. Redadmin checked with Chuprov to see if he was willing to take the risk, but Chuprov flatly refused. The client, however, tried to game the system—Morgenshtern was a stage name, and at the time, the singer's legal surname was Valeev. The client paid for a lookup on "Valeev," Chuprov fulfilled the order, but at the last minute, Redadmin decided to double-check. Realizing what the client had done, he withheld the file. A similar incident happened with PDE: among a batch of names someone ordered from him was the head of a federal arbitration court department. "What the hell is this? Vet your orders. I'm not handing that one over. Why should I pay an employee for this? And it's not the first time," he snapped at the client.

As long as they followed the rule of not touching public figures, PDE and Redadmin faced almost no real risk. Chuprov and his police superior, Borisov, were in a more vulnerable position—but the money seemed to make the risk worthwhile.

"The Roof Is Leaking"

At the end of 2004, journalists from *Forbes Russia* bought a disc in Moscow containing income data for nearly seven million residents of the capital and surrounding region—including top government officials and celebrities. The authorities shrugged it off. “We have no evidence that our databases are being sold. But if it’s true—well, that’s very bad,” said the deputy head of the tax service for the Central Federal District, with a hint of fatalism. The Interior Ministry’s cybercrime division, Department "K", added that no investigation into the leak was underway.[27]

A year later, the same thing happened again: reporters bought another database at a Moscow radio market containing income records for residents of the capital region. In all likelihood, the data in both cases came from the same source—reportedly the head of a department at the tax service, who allegedly walked the database out of the office on a hard drive. The “mole” was quietly fired, but the agency decided not to alert law enforcement—better to keep it in the family. The sellers weren’t so lucky. In late 2005, police and FSB officers made a show of arresting those duplicating and distributing the discs (several tens of thousands were seized).[28] But the crackdown barely scratched the surface of the market: the leaked database could still be ordered in Moscow and delivered right to your office—for just 1,000 rubles

[27] The Database Was Leaked // https://www.forbes.ru/forbes/issue/2004-12/21879-bazu-sdali?ysclid=lzic22cdwb520344320

[28] The FSB Cracks Down on Leaked Databases // https://www.kommersant.ru/doc/627380

(around $30). All this while the mole—or moles—were rumoured to have made a fortune off the leak. [29]

This was one of the few public examples from the 2000s where a leak and sale of personal data prompted any response from the authorities. In the archive Vasily sent me for free in 2017, there are hundreds of databases from that era—but only a handful of cases where anyone was actually punished for data theft. In part, that's because of the same logic that let the tax official off the hook: better to quietly fire someone than to take the matter to court and risk public scandal. And without a formal complaint from a victim—whether a government body, private company, or individual—law enforcement often couldn't even open a case. For example, when the entire database of Central Bank transactions leaked online, the regulator chose not to go to the police, opting instead for an internal inquiry.

Private companies were a bit more proactive in dealing with data leaks. In 2009, Moscow law enforcement detained Ivan Shvaga, an employee of Rosgosstrakh (Russia's largest insurer, which had been privatised a few years earlier but kept its well-known brand). Shvaga had tried to sell a customer database stored on a flash drive for 50,000 rubles—around $1,400 at the time. Such a database was a hot commodity for brokers: it allowed them to cold-call potential clients with tailored insurance offers, already knowing what assets they owned and how much they were willing to pay to protect them. Shvaga looked for buyers on broker forums—unaware that his company's own security team was monitoring them. They quickly reported him to the police. At trial, Shvaga expressed remorse and pleaded hardship: he had come to Moscow from Moldova to earn a living, was living alone, received no support from his family, and was struggling financially. The court sentenced him to a year in a penal settlement.[30]

[29] Confidential Data Leaks: 5 Russian Scandals of 2005 // https://www.cnews.ru/reviews/free/2005/articles/conf/
[30] Legal Case Opened Over Customer Database // https://www.kommersant.ru/doc/1173217

When no obvious victims were in sight, the authorities looked for them among their own ranks. In the mid-2000s, security officers in Perm detained 23-year-old Vyacheslav Oborin, who had been selling databases online. His offerings included the mobile numbers of local residents, details on regional business figures, and personal data of traffic police officers in the Perm region. Veterans of the Interior Ministry and the FSB stepped forward as the injured parties. "Criminals we helped put behind bars could come after us. Our data should be protected—not sold for nine thousand rubles," they told the court. Their grievances proved sufficient to land Oborin a suspended sentence.[31]

At the same time, their active-duty colleagues were busy *protecting* the market—after all, discs containing highly sensitive information couldn't have been sold without the knowledge of law enforcement. "Aren't you afraid that I might be from the police and arrest you right now?" a *Komsomolskaya Pravda* reporter asked the owner of a stall at one of Moscow's radio markets in 2006. "You? From the police? Sorry, but no one's warned me about you! Let the ones with a leaky roof worry," the seller shot back, hinting that his own "roof"—criminal slang for protection—was firmly in place.[32] It could've been dismissed as a joke, but a decade later Vasily, who was still openly selling databases, boasted to me about contacts in the Moscow police who, he claimed, could help him out if he ran into legal trouble. Just how far up that "roof" extended is unclear. Russian cybersecurity expert Ashot Oganesyan, who has followed the data black market for years, believes that for a long time authorities simply looked the other way. "It was as if the whole thing existed in a parallel reality," Oganesyan muses. "Then, sometime in the 2010s, a kind of cover emerged—and only after that did a real crackdown begin."

[31] *Megapolis* Distributor Given Suspended Sentence // https://www.kommersant.ru/doc/588011
[32] Who Steals Databases—and How? // /https://www.kp.ru/daily/23667.4/50491/

In the summer of 2011, the FSB suddenly made a loud announcement: it was going to put an end to the open sale of databases containing personal information.[33] A follow-up report soon boasted that raids on three of Moscow's radio markets had led to the seizure of over 15,000 discs—and along with personal data, some of them even contained classified state information. The crackdown lasted all summer. In the end, disc sales didn't stop altogether, but sellers became more cautious, keeping a lower profile. Two years later, Georgy Alburov—an investigator with Alexei Navalny's Anti-Corruption Foundation—went looking for leaked databases. He didn't manage to buy anything. "Everyone treated me with suspicion—apparently, I looked like the kid in movies trying to buy a porn mag," he recalled. "In the end, I just downloaded the database I needed from torrents."

Gradually, the niche once occupied by discs full of increasingly outdated leaks was overtaken by the *probiv* market—the trade in live, real-time data lookups. That's where police officers, government clerks, bank employees, and telecom workers now turned in hopes of cashing in on their access to personal data, just like Ivan Shvag from Rosgosstrakh once had. But the risks had grown: law enforcement now found it much easier to catch not the middleman hiding behind a Telegram nickname, but the actual police officer or bank clerk leaking the data. All it took was a "test purchase"—placing a fake order and then checking internal systems to see who accessed the file.

In 2019, while working on an investigation into the *probiv* market for the BBC Russian Service, I reviewed over a hundred court cases ending in convictions. On average, several dozen people ended up on trial each year for selling personal data. In nearly every case, they were

[33] The FSB intends to completely suppress illegal sale of databases in Russia // https://rg.ru/2011/06/25/baza-anons.html

employees of private companies: security staff at telecom firms and banks also kept an eye on the forums, tracked down suspicious offers—and then filed reports with the police.

For example, in the autumn of 2018, a young man from Ryazan named Mikhail Kudukhov was sentenced to 240 hours of community service—he worked at the mobile operator MTS and had sold data on the owners of seven phone numbers from other regions. Alexander Chernyshov, an employee at the Nizhny Novgorod branch of Sberbank, got off with a mere 10,000-ruble fine, even though he had sold data on at least 11 people—and received payment straight to his own Sberbank card. You could go on listing such cases, but the pattern is always the same: the punishments were mild, and the number of data lookup offers on the market stayed consistently high.

Employees of government agencies were punished even more rarely—I found only a handful of such cases. In 2019, for instance, two brothers, Alexei and Artyom Pugachev, who worked in a district police department in the Nizhny Novgorod region, were caught selling data. They earned at least 800,000 rubles and got off with suspended sentences of a year and a half. Justice was even more forgiving to the deputy head of the tax office in the town of Vidnoye near Moscow: he received only a fine and was granted amnesty in honour of the 70th anniversary of Victory in the Great Patriotic War.

As Ashot Oganesyan explained to me at the time, only a small fraction of those caught selling data ever ended up in court. The offence wasn’t considered particularly serious, investigators were reluctant to take on such cases, and companies, as before, were in no rush to report their "moles." By the mid-2020s, the situation had shifted slightly: convictions for bank data breaches had become almost nonexistent (likely because banks preferred to quietly dismiss employees rather than stir up scandal), employees of mobile providers still typically received

suspended sentences or fines, but the sale of information from government databases was being punished more frequently—and more harshly.

In general, just like in the 2000s, the law enforcement machine only really starts moving after a major scandal. For example, in the autumn of 2018, following Bellingcat's investigation into the Skripal poisoning, the security services quickly detained specific border service officers who had sold data on GRU officers Chepiga and Mishkin to Christo Grozev. That shook the market for a while: data providers grew wary of taking new orders, fearing law enforcement attention. But by spring 2019, everything was back to business as usual—and I was able to buy data on the breach with ease, as part of a journalistic experiment.

PDE and Redadmin—the data brokers—seemingly had little to worry about. Even if police officer Kirill Chuprov had been caught red-handed, it was unlikely the investigation would lead back to them. In all the criminal verdicts I reviewed, intermediaries were usually referred to as "unidentified individuals": law enforcement had no incentive to track them down if the person leaking the data had already confessed and the case could be pushed through to court.

"In the data-trading chats, people would say that someone got nabbed from time to time. Apparently, they'd sold info on the 'wrong person'," Alexei recalls. By helping uncover the FSB poisoners, he and his partner had pierced a whole cluster of the *wrong* people.

Face Down in the Snow

In the summer of 2019, central Moscow was seething with protest: rallies erupted over the authorities' refusal to allow independent candidates to run for the city's parliament, the Moscow City Duma. Alexei Navalny was the driving force behind the demonstrations, though the authorities tried to neutralise him—at one point detaining him during his morning jog on the eve

of a rally. His running skills came in handy for his supporters too: police and the National Guard chased protesters through the streets, and people hid wherever they could—once, a group even sought refuge in a church. Among those fleeing the batons was Alexei—not yet a data trafficker, just an unemployed man. Though short on money, he made a point of travelling to Moscow for the protest. And by his account, it was worth it: he and his friends managed to escape the police by ducking into a café.

The future Redadmin began watching Navalny's investigations while still serving in the army: the politician was exposing corruption that outraged even rank-and-file conscripts. Alexei attended his first-ever protest back in his hometown in 2017, after Navalny released an investigation into the lavish lifestyle of former president and prime minister Dmitry Medvedev. The revelations sparked such widespread anger that spontaneous rallies broke out across the country. In Alexei's provincial hometown, 500 people showed up—a striking turnout for such an apolitical backwater.

Alexei followed not just Navalny's speeches, but also Bellingcat's investigations into the downing of the Malaysian airliner. At the same time, he was hearing stories from friends—they'd served in the military in the Rostov region, near the Ukrainian border, and had seen the bodies of Russian soldiers being brought back from Donbas. "On TV they were saying Russia had nothing to do with the conflict in eastern Ukraine, while Western media insisted otherwise," Alexei says. "To me, it looked like this: the same corrupt government Navalny was exposing was carrying out an aggressive war on foreign soil."

Christo Grozev was incredibly lucky that one of the data brokers he worked with happened to be Alexei. For a long time, they knew each other only as anonymous contacts on Telegram, speaking strictly about business. One day, while checking Grozev's latest order for

any high-profile names, Alexei noticed a few linked to the MH17 case. "Huh, interesting guy," he thought about the client—but he kept filling the order. "If it weren't for my opposition views, I would've turned it down," he explains. "There are other ideologically driven people in the data trade, like cops who were more than happy to run checks on pro-Putin types."

After recognising—on the second pass—that Navalny's poisoners were among the names in his orders, Redadmin finally figured out who was behind the anonymous Telegram account. "Good afternoon, Christo! That was an amazing investigation," he messaged the Bulgarian journalist. Christo didn't play coy—he immediately asked if Alexei needed any help. Alexei turned him down. "I didn't think they'd trace it back to us so quickly," he recalls.

Just like after the Skripal poisoning exposé, the investigation into the attempt on Navalny's life sent the security services into overdrive. They launched a hunt for whoever had sold the data, internal checks began, and Kirill Chuprov went to ground. A week later, he messaged his partners from a fresh anonymous account: "The heat's dying down. We're back in business on Monday." Chuprov was wrong—just a few days later, they were arrested.

Identifying the police officer was laughably easy: all investigators had to do was check in *Rospasport* who had pulled passport records on the FSB officers named in Navalny's investigation. Chuprov didn't resist much, but insisted he'd been pressured into selling the data by his boss—Major Borisov. From Chuprov's QIWI wallet, investigators quickly traced payments to Alexander (aka PDE), who had been transferring money to Chuprov and other insiders. Since QIWI is a Russian payment service, the company responded to law enforcement requests with detailed account information. It turned out the wallet was registered to a childhood acquaintance of Alexander's from the same hometown. QIWI also handed over a list of IP addresses used to access the wallet. The most common one? Alexander's home IP. Like Chuprov,

he didn't deny anything during questioning. Alexander understood how serious things were from the first encounter: he was grabbed on the street near his home and thrown face down into the snow. During the apartment search, they kept him pinned to the floor.

His partner Alexei, aka Redadmin, didn't come under immediate investigation. When he learned of his friend's arrest, he managed to delete all the work chats in time. Alexander also got off relatively lightly—he was released during the investigation, and in late January 2021, the two friends even attended a protest in support of Navalny in their hometown. The opposition leader had just returned from Germany, where he'd been recovering after the poisoning, and was arrested immediately upon arrival at the airport. Demonstrations swept across Russia, and the data brokers joined the crowds, hoping the wave of protest might lead to real change. Both would end up disillusioned—especially Alexander, who until then had never attended a political rally in his life.

Naturally, they stopped doing any further "probiv" work. Ironically, one of the last requests that came to Alexander was for the phone billing records of Maria Pevchikh—a close associate of Navalny who had spent years conducting investigations with him. Before the poisoning, she was known only to a small circle of journalists. Pevchikh had accompanied Navalny on his trip across Russia when the FSB tried to kill him, and pro-Kremlin propaganda later attempted to frame her as a kind of Western intelligence agent embedded in the opposition leader's inner circle. It's possible the billing data had been ordered by some Kremlin-adjacent media outlet: the request came through an intermediary. Alexander, however, flatly refused to take it on—not so much for political reasons, but because of the informal rule: *don't probe high-profile people*.

The investigators hardly ever mentioned the names of Navalny's poisoners when speaking with Alexander—they came up only once, briefly, during an interrogation, and even then without any mention of where the men worked. In fact, no victims were needed for the criminal case at all. Alexander was charged with offering a bribe in exchange for access to internal Ministry of Internal Affairs databases, while the police officers, Chuprov and Borisov, were charged with accepting that bribe. I examined the chat screenshots that investigators had extracted from Alexander's devices—they clearly show who was buying information from him, and about whom. In some cases, both the clients and the targets were easy to identify. I reached out to several of them, and all responded the same way: they had never heard anything about the case, and no one had contacted them. The investigators' reluctance to dig any deeper is easy to understand. The suspects had confessed, and the people whose names had been used to register the QIWI wallets confirmed everything. All that was left was to pad the file with a few supporting documents and send it off to court.

Better Not to Come Back

At the end of March, Alexei went to visit his former partner. On the way, he stopped by a nearby shop to pick up some pastries. *"What should I get you?"* he asked on Telegram. His friend replied with a short list. The shop was close to the apartment, and within minutes Alexei was at the door with the bag in hand. Since they'd literally been chatting just ten minutes earlier, he didn't bother to call or knock—he simply messaged, *"Open the door."* There was no reply. That was strange enough. But what was even stranger: Alexander's glasses were lying outside the door.

Alexei decided to call his friend's wife. She wasn't home, but she suggested he come pick up the keys so he could go back and figure out what was going on. While talking to her, Alexei stepped out onto the stairwell balcony and noticed a white van parked near the building. He knew every car that usually came through this courtyard—but this one, he'd never seen before.

After the call, Alexei went back to the stairwell and started ringing his friend again. Eventually, he got a reply—a generic message: *"Sorry, I can't talk right now."* That struck him as odd. For security reasons, they never used regular calls or texts—unlike encrypted messengers, those could easily be monitored by Russian law enforcement. Alexei replied with a warning: *"I'm calling the police."* That seemed to do the trick. The door opened. But it wasn't Alexander standing there. Two men in camouflage and balaclavas stepped out of the apartment. No insignia, no badges—nothing to show who they were. Still, Alexei is certain: they looked exactly like FSB agents do in the operational footage you see on TV.

"Who are you?" one of them asked.

"And who are you?"—Alexei replied defiantly. A second later, they were already shoving him into the apartment.

Alexander was sitting on the floor, his head and eyes bound tightly with duct tape. When Alexei tried to protest, he was met with a punch to the gut. They taped his eyes too—and shoved a dirty potato from a sack in the hallway into his mouth to shut him up. From that point on, they were treated like baggage: thrown into the same white van and driven off to an unknown destination. Judging by the voices, there were several men involved. "They must've come for Sasha while I was walking back from the shop," Alexei reflects now. "He probably thought it was me at the door, opened up, they hit him—and that's when his glasses fell." As he tells the

story, he sometimes lets out a nervous laugh. It's clear that part of him still struggles to revisit that day—but another part feels the need to get it out.

"I wasn't scared. Mostly, I was thinking about how the hell to get out of there," Alexei says. During the ride, the men in camouflage pulled the potato out of his mouth and started questioning him: what was he doing at Alexander's place? Alexei stammered that he'd just come to visit, that he made his living trading crypto, and that he had no idea why he was in the van. They began to search him. In his pocket was a smartphone—and fearing he might be forced to unlock it under threat of torture, the ex-data cracker grabbed it and snapped it clean in half.

"Idiot! Why the hell did you break your phone?!"

"What if you steal my crypto?" Alexei shot back.

Once they'd emptied his pockets, the van came to a halt. Alexei was shoved out onto the road and forced to his knees. For a moment, he was sure they were going to kill him. "Please don't shoot!" he begged. "Count to 25 and stand up," one of them ordered. He did as he was told, and soon heard the van drive off. After a few moments, he tore off the duct tape and looked around. He was in a village, several dozen kilometres from his hometown. His belongings had been tossed onto the road. His cash had been ripped into tiny pieces—clearly to slow him down, make it harder to get back home. He had no choice but to flag down passing cars and ask for help, explaining to drivers that he'd been kidnapped and dumped in the middle of nowhere.

A few hours later, exhausted and shaken, Alexei was at the police station recounting everything that had happened to him and his friend. At the same time, Alexander's wife was writing a missing person report. According to Alexei, the police were already preparing to issue a citywide alert to intercept the white van—when two plainclothes men walked into the office. They flashed their FSB badges and asked Alexander's wife to come with them for a search. Her

half-written report went straight into the bin. The alert was cancelled. She was driven to her parents' apartment. The search record confirms that the operation took place at an unusual hour—in the evening. Russian security forces usually prefer to show up at dawn, rattling the doors of half-asleep targets.

The whole time, Alexander was being interrogated somewhere in the woods—if you could call it that. According to him, he was on his knees beside a pit while his captors fired warning shots into the air, threatening that the next one would go straight through his head. Why such theatrics were necessary, given that Alexander had already confessed during the investigation, remains unclear. Perhaps the authorities suspected he wasn't just a hired hand selling data in ignorance, but a true believer—a willing member of Christo Grozev's team. Alexei adds that, while he was still in the van, he overheard two of the men speaking in Chechen and dropping the name of Ramzan Kadyrov, the president of Chechnya—a man infamous for brutal methods and who proudly calls himself "Putin's foot soldier." It's possible the Chechen authorities had dispatched their own specialists to help local operatives with the art of extracting confessions.

Later that evening, around nine o'clock, Alexander was brought to the Investigative Committee. In one of the case file photographs, he is seen "voluntarily"—as the caption claims—handing over two phones, his face a mask of exhaustion and stone. Meanwhile, his friend was already writing to Christo Grozev: this time, he really did need help. The Bulgarian investigator offered to get him out of the country, and Alexei agreed. The next day, he applied for a new internal passport. Then came the wait—for international passports to be issued for the whole family: his elderly mother, his adult sister, and his younger brother. In the spring of 2021,

the four of them—none of whom had ever left Russia before—boarded a flight to Yerevan via Moscow, and from there continued on to Kyiv. They were leaving not for vacation, but for exile.

"Better not come back," his acquaintances warned him soon after he left. His former partner Alexander was sentenced to three years in a high-security penal colony. The police officers, Chuprov and Borisov, received even tougher sentences—four and a half years and eight years behind bars, respectively.

In Kyiv, Alexei met Grozev in person for the first time. The Bulgarian journalist admitted frankly that he hadn't expected the data broker to actually leave Russia. "Alexei is a genuinely inspiring example," says Christo. "He eventually realised who he'd been selling data to—and not only didn't back away from the work, but was even ready to do it for free." From Ukraine, Grozev arranged for Alexei and his family to relocate to a European country and helped them with their paperwork. I spoke with Alexei's relatives—kind, down-to-earth people who take what happened to them in quiet stride.

On 16 February 2024, news broke that Alexei Navalny had died in a Russian penal colony in the Far North. It happened to be the very week I was meeting with Alexei—the former data broker—for this book, and we visited a spontaneous memorial set up in the politician's memory. Alexei lit a candle and stood in front of Navalny's portrait for a long time. You could tell just how personal this loss was for him. He often says that Navalny "sort of" knew who he was—and that his name, under a pseudonym, appears in the credits of the documentary *Navalny*.

"I think I've balanced out some of my karma by helping good people—and Navalny himself," Alexei says when I ask again about the harm he might have caused by selling personal data. Shortly after leaving Russia, still clearly shaken by everything that had happened, he wrote

an open letter about his past, about Navalny, and about how he views Putin's Russia. He never ended up publishing it, but he showed it to me. One part reads:

"I'm just an ordinary guy from the Russian backwoods who—like my friend Alexander—unfortunately got into the wrong line of work. We never wished harm on anyone. We ended up in this market simply because we couldn't pay the bills, and there were no real opportunities to earn or realise ourselves in our region. There was no malicious intent behind what we did—I'll be honest: we were just in it for the money."

These days, Alexei makes a living helping Christo Grozev and independent Russian media in exile. He no longer works with corrupt police officers directly—instead, he buys data from former contacts on the black market, using it strictly for journalistic investigations. At one point, he even had the idea to build a Telegram bot that would let reporters more easily search across leaked databases. But he eventually dropped it: what if scammers, security operatives, or other typical clients of such tools started using it? Those people, he decided, he no longer wanted to help.

This book is supported by the **Straight Forward.**

The Straight Forward is an anti-dictatorial and anti-war initiative for promoting freedom of speech. We amplify the voices of Russian authors whose literary works face insurmountable barriers within their homeland due to oppressive censorship and pervasive risk of political imprisonment. SF supports courageous non-fiction writers and distributes their manuscripts among a worldwide network of established publishers who share our commitment to tell true stories and to enlighten societies about dangers of autocratic regimes.