RKS Global

April 2026 · rks.global

Detecting Surveillance in 30 Popular Russian Apps

Method: static APK analysis (decompilation, search across 68 surveillance checkpoints in 12 categories)
Sample size: 30 apps from RuStore and Google Play

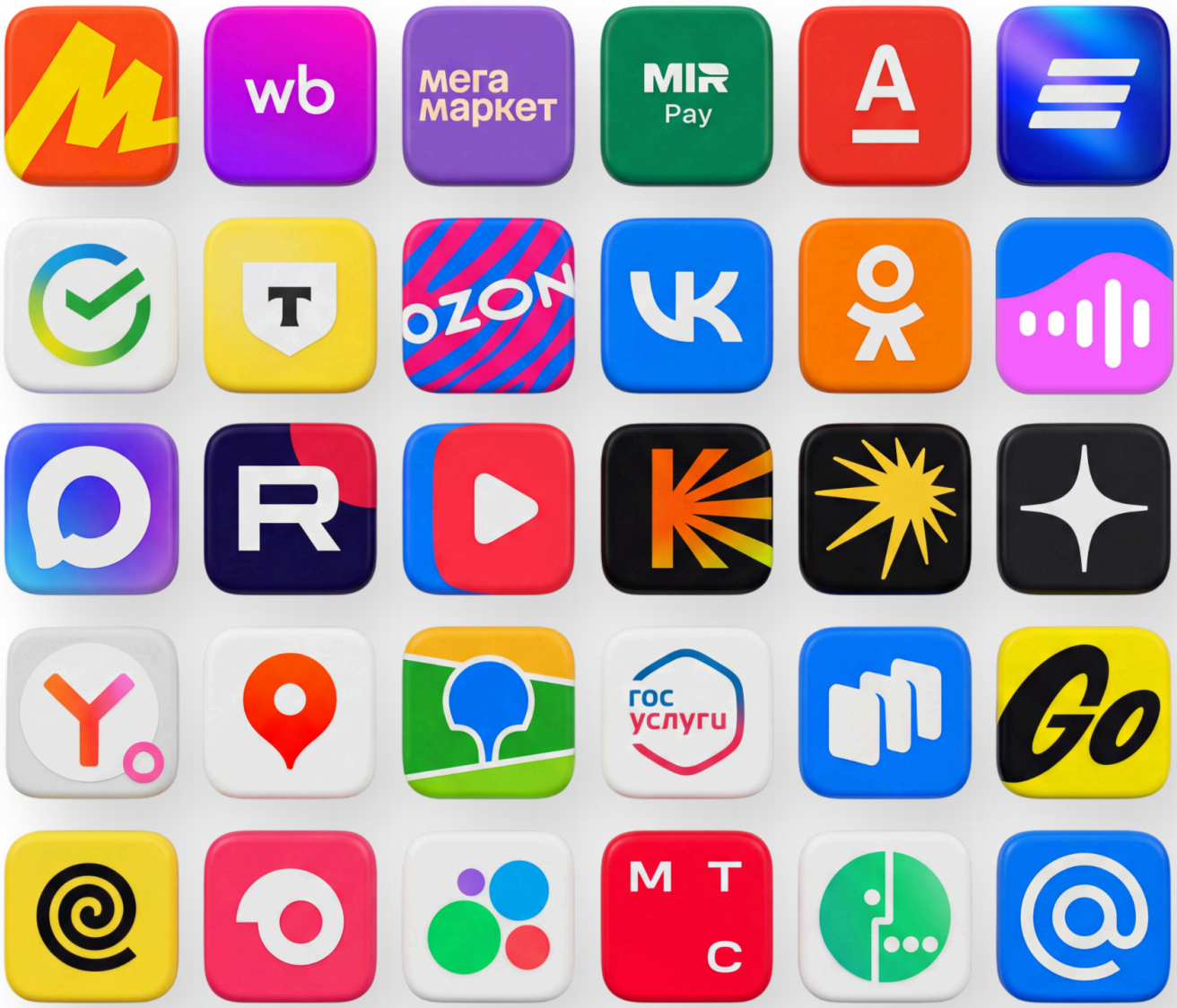

Table of contents

Key Findings

- 22 out of 30 apps detect VPN, of which 19 are confirmed to send VPN status to a server
- 29 out of 30 apps check for root access (all except Yandex Go)
- 24 out of 30 request microphone access
- 28 out of 30 request camera access
- 24 out of 30 send the list of installed apps to their servers
- 11 out of 30 apps received a RED rating (maximum surveillance)
- 49 out of 68 surveillance checks operate without user interaction — immediately after installation

The analysis database is available at this link.

1. Which Apps Monitor VPN Usage? (22 out of 30)

What This Means

When an app detects VPN, it records that the user is hiding their real IP address. This information can be transmitted to the company's servers, and, from there, can be accessed by law enforcement agencies upon request.

VPN Detection Methods Used by Apps

Method	What it does	Number of apps
TRANSPORT_VPN	Direct API call to Android: "is VPN enabled?"	16
Network interfaces tun0	Enumerating network adapters — VPN creates a virtual tun0	14
Reading /proc/net/tcp	Low-level reading of Linux kernel network tables to detect VPN ports	4
Proxy settings check	Reading system properties http.proxyHost	9
Sending VPN status to server	VPN flag transmitted in telemetry	19
Tor detection	Searching for packages org.torproject.torbrowser	1

App Ranking by Depth of VPN Surveillance

App	Detection methods	What exactly it does
Yandex Browser	**4**	TRANSPORT_VPN + /proc/net/tcp + tun0 + **детект Tor** + **→server**
Yandex Maps	**4**	TRANSPORT_VPN + /proc/net/tcp + tun0 + proxy
VKontakte	3	TRANSPORT_VPN + tun0 + proxy + **→server**
My MTS	3	TRANSPORT_VPN + tun0 + proxy + **→server**
Sberbank Online	3	TRANSPORT_VPN + tun0 + proxy + **→server** (`setVpn()` в clickstream)
T-Bank	3	/proc/net/tcp + tun0 + →**server** (isVpnConnected в fingerprint)
VK Video	2	TRANSPORT_VPN + proxy + **→server**
Wildberries	2	tun0 + proxy
Kinopoisk	2	TRANSPORT_VPN + tun0 + **→server**
Ozon	2	TRANSPORT_VPN + proxy + **→server**
Samokat	2	TRANSPORT_VPN + tun0 + **→server**
RuStore	2	TRANSPORT_VPN + proxy + **→server**
VTB Online	2	TRANSPORT_VPN + tun0 + →**server** (is_vpn_on в NetworkSettingsDto)
Yandex Music	2	/proc/net/tcp + tun0
VK Music	2	TRANSPORT_VPN + tun0 + →сервер (is_vpn в каждом stat-событии)
Avito	1	TRANSPORT_VPN + **→server**
Alfa-Bank	1	proxy + **→server**

App	Detection methods	What exactly it does
2GIS	1	TRANSPORT_VPN + →**server**
MegaMarket	1	tun0 + →**server**
Odnoklassniki	1	TRANSPORT_VPN + →**server**
MAX	1	TRANSPORT_VPN + →**server**
Rutube	1	tun0 + →**server** (VpnStatusResponse API)

Apps That Do NOT Detect VPN (8 out of 30)

Total: 8 out of 30 apps do not detect VPN.
Yandex Market, Yandex Eda, Mail.ru Mail, MegaFon, Mir Pay, Gosuslugi, Yandex Go, Dzen.

Conclusion: Yandex Browser is the only app that searches for Tor on the device. Yandex Browser and Yandex Maps use the maximum number of VPN detection methods (4 out of 6). **19 out of 22** apps with VPN detection are confirmed to send VPN status to their servers — including T-Bank (@SerialName("isVpnConnected")), Sberbank (clickstream analytics), VTB (@SerializedName("is_vpn_on")), Yandex Browser (vpn_enabled in telemetry) and Rutube (VpnStatusResponse API). MAX **obfuscates** network interface names (tun/ppp/tap/pptp0 are encoded as byte arrays), indicating deliberate concealment of VPN detection from researchers.

2. The Most Aggressive Apps by Overall Surveillance

Ranking by number of triggered checks out of 68:

#	App	Rating	Score	VPN	VPN → Server	Key finding
1	**Т-Банк** Bank	RED	**65/68**	3	yes	Searches for Frida via /proc/net/tcp:27042, `isVpnConnected` in fingerprint
2	**MegaMarket** Маркетплейс	RED	**65/68**	1	yes	GPS every 2 sec, com.group_ib.sdk, contacts+SMS+call log
3	**VKontakte** Social network	RED	**64/68**	3	yes	IMEI/IMSI via reflection (Android 10 bypass), contact sync
4	**Odnoklassniki** Social network	ORANGE	**64/68**	1	yes	DeviceAdmin hidden in "emoji" module
5	**Sberbank Online** Bank	RED	**64/68**	3	да	Touch data: X/Y/pressure/size, VPN in clickstream
6	**Yandex Browser** Browser	RED	**63/68**	4	yes	Tor detection + `vpn_enabled` in telemetry + WhoCalls
7	**Yandex Maps** Navigation	ORANGE	**60/68**	4	?	VPN detection in proprietary code (not SDK)
8	**VTB Online** Bank	RED	**59/68**	2	yes	`is_vpn_on` in NetworkSettingsDto → diagnostics server
9	**Rutube** Video	ORANGE	**57/68**	1	yes	Fraud SDK sends app list + `VpnStatusResponse` API
10	**Alfa-Bank** Bank	ORANGE	**56/68**	1	yes	Kaspersky SDK reads ALL notifications

#	App	Rating	Score	VPN	VPN → Server	Key finding
11	**My MTS** Telecom	RED	**56/68**	3	yes	ACCESS_SUPERUSER in manifest, MTS GEO SDK
12	**Ozon** Marketplace	RED	**56/68**	2	yes	247 banks + contacts in JSON → WebView
13	**Wildberries** Marketplace	RED	**55/68**	2	?	Background clipboard interception + full call log
14	Samokat Delivery	RED	54/68	2	yes	List of VPN apps — in a food delivery app
15	Kinopoisk Streaming	ORANGE	53/68	2	yes	vpn_enabled + GPS sent to server
16	RuStore App Store	RED	53/68	2	yes	An app store that surveils VPN
17	Yandex Music Music	ORANGE	53/68	2	?	Frida detection in a music player
18	VK Music Music	ORANGE	52/68	2	yes	tun0 + TRANSPORT_VPN, is_vpn in every stat event, russian_trusted_root_ca
19	VK Видео Video	ORANGE	51/68	2	yes	3 SDKs search for VPN, contacts → vk.com
20	2GIS Navigation	ORANGE	51/68	1	yes	80+ banks + contacts via JNI → native code
21	Gosuslugi Gov. services	ORANGE	51/68	—	—	Keystroke timing in a government app
22	Dzen Media	ORANGE	49/68	—	—	GPS every 2 sec for a news feed
23	Yandex Eda Delivery	ORANGE	48/68	—	—	Triple geolocation: GPS + cell towers + WiFi
24	Avito Classifieds	ORANGE	46/68	1	yes	~200 third-party packages in manifest queries

#	App	Rating	Score	VPN	VPN → Server	Key finding
25	MAX (TamTam) Messenger	ORANGE	46/68	1	yes	VPN names obfuscated with byte arrays
26	MegaFon Telecom	ORANGE	41/68	—	—	Contacts uploaded every 24 hours
27	Yandex Market Marketplace	ORANGE	40/68	—	—	is_rooted in every HTTP request
28	Mail.ru Mail Email	ORANGE	40/68	—	—	Server decides which apps to search for
29	Yandex Go Taxi	ORANGE	39/68	—	—	No VPN/root detection — the only one out of 30
30	Mir Pay Payments	ORANGE	35/68	—	—	99% of code hidden behind libprotector.so

Category Leaders

Banking apps are the most aggressive group. T-Bank (65), Sberbank (64), and VTB (59) rank among the top 10. All three send VPN status to servers, use extended device fingerprinting, and detect root access and analysis tools.

VK ecosystem — VKontakte (64), Odnoklassniki (64), VK Video (51). United by VK Push SDK, ok.tracer, MyTracker. VKontakte and Odnoklassniki have one of the most extensive background infrastructures (67 and 77 services respectively).

Yandex ecosystem — Browser (63), Maps (60), Kinopoisk (53), Music (53). United by AppMetrica, AppsFlyer. Yandex Browser is the only app with Tor detection and transmits `vpn_enabled` to analytics.

Marketplaces — MegaMarket (65), Ozon (56), Wildberries (55). MegaMarket (owned by Sber) shares first place with T-Bank, it uses the com.group_ib.sdk, and collects contacts, SMS, and call logs.

Conclusion: T-Bank and MegaMarket are the surveillance leaders with 65 out of 68 detected checks.

3. Unexpected Surveillance Methods

3.1. Reading /proc/net/tcp — Scanning Kernel Network Connections

Apps: T-Bank, Yandex Browser, Yandex Maps, Yandex Music

These apps read the `/proc/net/tcp` file — the Linux kernel's TCP connection table. They search for port `0x69A2` (27042) — the default port for Frida, a reverse engineering tool. Essentially, the app checks whether someone is analyzing it right now. This is something an ordinary user would never expect from a banking app or a navigation tool.

3.2. Touch Timing — Behavioral Biometrics

Apps(11): T-Bank, Alfa-Bank, 2GIS, Yandex Eda, MegaMarket, My MTS, Odnoklassniki, Gosuslugi, Rutube, Sberbank Online, Yandex Music

They intercept `dispatchTouchEvent()` —every screen touch with coordinates, pressure, and timing. Sberbank stores `TouchData` objects with fields `pressure`, `size`, `x`, `y`. The com.group_ib.sdk (in Alfa-Bank, MegaMarket, My MTS) intercepts all touch events.

Why this is unexpected: behavioral biometrics allow identifying a person by how they press the screen — even without logging in. Rutube records touch coordinates, despite being just a video hosting platform.

3.3. Frida and Xposed Detection — Anti-Reverse Engineering

Apps: T-Bank, Yandex Browser, Yandex Music, Yandex Maps

They search for traces of Frida (a dynamic analysis tool) by:
- Reading `/proc/<pid>/maps` and searching for the string `frida`
- Checking `/proc/net/tcp` for port 27042

Why this is unexpected: apps actively resist attempts by users or researchers to analyze their behaviour. Yandex Maps — a navigation app — is protected as if it were military software.

3.4. List of VPN Apps — Samokat and MegaMarket

Apps: Samokat, MegaMarket

They use queryIntentServices("android.net.VpnService") — obtaining a list of all VPN apps installed on the device. Not just "is VPN enabled," but which specific VPN programs are present.

Why this is unexpected: a food delivery app (Samokat) and a marketplace (MegaMarket) know which VPNs you have installed.

3.5. Tor Detection — Yandex Browser

App: Yandex Browser

The only one out of 30 apps that explicitly searches for Tor Browser packages: org.torproject.torbrowser, org.torproject.torbrowser_alpha.

Why this is unexpected: a browser that itself offers an "Incognito" mode searches for an anonymity tool on your device.

3.6. Scanning 200+ Third-Party Apps — Avito

App: Avito

The <queries> block in its manifest lists more than 200 packages — banks (Sberbank, T-Bank, VTB, Alfa), marketplaces (Ozon, Wildberries), social networks (VK, Telegram, Instagram, Facebook), services (Yandex), and competitors (Drom, CIAN, HH.ru). Avito can determine which of these apps are installed.

3.7. Ozon Knows Whether You Have AnyDesk and TeamViewer

App: Ozon

Contains a hardcoded mapping: com.anydesk.anydeskandroid → "AnyDesk", com.teamviewer.quicksupport.market → "QS". Samokat has a similar list. These apps can check for the presence of remote control software.

3.8. Total Device Fingerprinting

29 out of 30 apps check for root access (all except Yandex Go). **24 out of 30** check whether a debugger is attached. **24 out of 30** detect emulators.

What this creates: a unique device "fingerprint" that allows tracking the user even after reinstalling the app.

Tracker SDKs — Who Is Watching Everyone

SDK	Number of apps	Presumed owner
Yandex AppMetrica	17	Yandex
MyTracker	14	VK (Mail.ru)
AppsFlyer	10	Israel
Huawei HMS	9	Huawei (China)
Firebase Analytics	8	Google
Sentry	8	Sentry (USA)
VK Push SDK	6	VK
SDK com.group_ib.sdk	3	Group-IB (Russia)*

* **Update as of April 16, 2026:** A representative of Group-IB has informed the RKS Global team that Group-IB divested and fully exited the Russian market in April 2023, and does not serve any clients in Russia or operate there.

Conclusion: AppMetrica (Yandex) and MyTracker (VK) are the two main Russian trackers embedded in more than half of the analyzed apps. Data from these SDKs is available upon request by Russian law enforcement agencies.

4. Which Permissions Work Without User Involvement?

Android divides permissions into two types:

- **Dangerous (runtime)** — require explicit user consent via a pop-up dialog
- **Normal (install-time)** — granted **automatically** upon APK installation, without any notification

4.1. "Silent" Permissions — Install-Time (Without User Consent)

These permissions form a surveillance infrastructure that **operates from the moment of installation**, before the user interacts with any permission prompts:

Permission	Apps	What this means for the user
RECEIVE_BOOT_COMPLETED	**30/30**	App automatically starts when the phone is turned on
FOREGROUND_SERVICE	**30/30**	App can run constantly in the background
QUERY_ALL_PACKAGES / <queries>	**27/30**	App can see all (or specific) installed programs on the device
SYSTEM_ALERT_WINDOW	**16/30**	App can draw over other apps
FOREGROUND_SERVICE_DATA_SYNC	**15/30**	Background data synchronization — a channel for sending collected data

Permission	Apps	What this means for the user
REQUEST_INSTALL_PACKAGES	**15/30**	App can install other APK files
REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	**12/30**	System cannot put the app to sleep — runs 24/7
FOREGROUND_SERVICE_MICROPHONE	**6/30**	Background microphone access without a visible app
FOREGROUND_SERVICE_LOCATION	**4/30**	Continuous background geolocation
FOREGROUND_SERVICE_MEDIA_PROJECTION	**4/30**	Background screen capture
FOREGROUND_SERVICE_CAMERA	**3/30**	Background camera access

What this creates in practice: he combination of RECEIVE_BOOT_COMPLETED (all 30) + FOREGROUND_SERVICE (all 30) + REQUEST_IGNORE_BATTERY_OPTIMIZATIONS (12) = the app starts on every phone boot, runs constantly in the background, and cannot be stopped by the battery saving system. **This entire infrastructure is installed without a single question to the user.**

4.2. Permissions Requiring User Consent (Dangerous/Runtime)

Permission	Apps	What the app gets
ACCESS_FINE_LOCATION	**30/30**	GPS coordinates accurate to meters
CAMERA	**28/30**	Photo and video capture
READ_CONTACTS	**28/30**	Full contact list

Permission	Apps	What the app gets
RECORD_AUDIO	**24/30**	Microphone recording
READ_MEDIA_IMAGES	**19/30**	Access to photos
WRITE_EXTERNAL_STORAGE	**16/30**	Writing and modifying files
ACCESS_COARSE_LOCATION	**14/30**	Approximate location
READ_CALL_LOG	**13/30**	Complete call history
ACCESS_BACKGROUND_LOCATION	**12/30**	Geolocation even when the app i closed
READ_MEDIA_VIDEO	**11/30**	Access to video recordings
WRITE_CONTACTS	**9/30**	Modifying contacts
READ_CALENDAR	**5/30**	Reading calendar events
READ_SMS	**5/30**	Reading all SMS messages
RECEIVE_SMS	**4/30**	Intercepting incoming SMS
SEND_SMS	**1/30**	Sending SMS without user knowledge

4.3. App Ranking by Number of Permissions

Note: full manifests were available for 5 out of 30 apps (T-Bank, VK Video, Alfa-Bank, Yandex Market, Yandex Eda). For the remaining 25, the count is based on permission mentions in analysis results and represents a lower estimate — the actual number of permissions may be higher.

#	App	Dangerous (with consent)	Normal (without consent)	Total
1	T-Bank	**23**	**24**	**47**
2	VK Видео	16	15	31
3	Alfa-Bank	13	17	30
4	Yandex Market	12	14	26
5	Odnoklassniki	16	9	25
6	Yandex Eda	10	14	24
7	MegaMarket	16	6	22
8	Sberbank Online	9	11	20
9	Avito	7	11	18
10	Yandex Browser	10	7	17
11	VKontakte	11	6	17
12	VTB Online	11	6	17
13	RuStore	10	7	17
14	2GIS	9	7	16
15	Dzen	9	7	16
16	My MTS	7	8	15
17	Mail.ru Mail	10	5	15

#	App	Dangerous (with consent)	Normal (without consent)	Total
18	Yandex Go	7	8	15
19	MAX (TamTam)	9	5	14
20	Ozon	9	5	14
21	Kinopoisk	6	7	13
22	MegaFon	7	4	11
23	Yandex Music	7	4	11
24	Gosuslugi	7	3	10
25	Mir Pay	3	6	9
26	Samokat	6	2	8
27	Wildberries	4	3	7
28	Yandex Maps	4	3	7
29	Rutube	6	1	7
30	VK Music	?	?	?

Conclusion: T-Bank requests 47 permissions — the most of all. Of these, 24 (including auto-start, background camera, microphone, and geolocation services, and APK installation) are granted **automatically without the user's knowledge**. Banking apps (T-Bank, Alfa-Bank, Sberbank) lead in the number of "silent" install-time permissions, forming a permanent background infrastructure.

Methodology

  - Static analysis: decompilation via apktool and jadx, search across 68 checks in 12 surveillance categories
- **Limitations:** static analysis only, without dynamic on-device testing
- check_failed **assessment**: 3 out of 2,400 cells (0.12%) could not be verified — VPN transmission for 3 apps (Wildberries, Yandex Music, Yandex Maps), where code is hidden in native libraries

APK versions

Package	Version
com.avito.android	v221.1
com.idamob.tinkoff.android	v7.31.1
com.vk.vkvideo	v1.139.1
com.vkontakte.android	v8.171
com.wildberries.ru	v7.5.6002-rustore
com.yandex.browser	v26.3.4.128
ru.alfabank.mobile.android	v12.46.05
ru.beru.android	v2026.10.2.c
ru.dublgis.dgismobile	v7.21.0.615.23
ru.foodfox.client	v3.120.0
ru.kinopoisk	v7.78.4
ru.mail.mailapp	v15.80.0.135859
ru.megafon.mlk	v4.63.0
ru.megamarket.marketplace	v6.2

Package	Version
ru.mts.mymts	v6.63
ru.nspk.mirpay	v1.60.4.350
ru.ok.android	v26.3.30
ru.oneme.app	v26.11.3
ru.ozon.app.android	v19.11.0
ru.rostel	v25.2.0.9435-rustore
ru.rutube.app	v31.4.4-rustore
ru.sbcs.store	v3.227.0
ru.sberbankmobile	v17.4.0
ru.vk.store	v1.98.0.1
ru.vtb24.mobilebanking.android	v20.5.0.3
ru.yandex.music	v2026.03.4 #140rur
ru.yandex.taxi	v5.67.3
ru.yandex.yandexmaps	v28.4.3
ru.zen.android	v26.3.4
com.uma.musicvk	v8.19

Surveillance Check Categories (12 Vectors)

#	Vector	Checks
S1	Enumeration of installed apps	6
S2	VPN/Proxy/Tor detection	7
S3	Device fingerprinting (IMEI/IMSI/MAC)	7
S4	Location tracking	5
S5	Network monitoring and telemetry	5
S6	Content access (contacts/SMS/files)	6
S7	Behavioral analytics (sensors/gestures)	6
S8	Audio/video surveillance	4
S9	Covert data exfiltration	6
S10	Anti-analysis protection (root/Frida/emulator)	5
S11	Russian legal context (SORM/Yarovaya Law)	4
S12	System persistence	7
	Total	**68**

Recommendations

Part 1. You Are in Russia

Threat model: data collected by apps is available to the FSB, MVD, and Investigative Committee — via SORM, the Yarovaya Law, and requests to companies. Data about a VPN app can lead to its being blocked.

App Isolation

24 из 30 приложений отправляют список ваших приложений на сервер. Если Сбербанк стоит рядом с VPN-клиентом — разработчики и силовики это знают.

- **Two phones** is the ideal option. One for Russian apps, and another for everything else.
- **One phone** — Android Work Profile via Shelter. Apps from different profiles cannot see each other: neither the app list, contacts, nor files. Work Profile does not hide VPN, it only isolates data between profiles, and therefore does not protect VPN apps.

VPN

Solutions (from best to simplest):

1. VPN on a router. Tunnel on the router, phone connects via Wi-Fi. Router with OpenWrt / Keenetic / Mikrotik + WireGuard or VLESS. Portable option — GL.iNet with VPN. Downside: only works on that router's Wi-Fi.

1b. Wi-Fi tethering from another phone. Same principle as VPN on a router, but the router is your second phone. Phone A has VPN + mobile hotspot enabled. Phone B (with Russian apps) connects to Phone A's Wi-Fi. Verification: on Phone B, visit an IP-checking website — if it shows the VPN server's IP, it works. Caveats: not all VPN clients route hotspot traffic through

the tunnel; some carriers restrict tethering; on Android 12+, there may be routing issues.

2. Two phones. Phone A, with VPN, is used for browsers, messengers, and accessing blocked sites. Phone B, without VPN, is used for Russian apps. No VPN is installed on Phone B. Downside: two separate digital environments for your life.

3. Split tunneling (partial solution). In some VPN clients, you can exclude Russian apps from the tunnel. Their traffic goes directly, but `tun0` remains on the device.
Downside: helps against some checks, but apps scanning for `tun0` can still detect VPNs.

4. Switching. Turn off VPN → open the app → force stop the app (Settings → Apps → Stop) → turn on VPN. It is important to actually stop it, not just minimize: all 30 apps run in the background and can detect the moment VPN is enabled. Downside: you need to remember everything.

Permissions — Revoke Now

Permission	Action
Geolocation	Only for navigation apps, only "while using."
Contacts	Revoke from all except messengers.
Microphone, camera	Only by request.
Call log, SMS	Revoke from all apps.

Background Activity

All 30 apps auto-start and run in the background. Restrict them: Settings → Apps → Battery → "Restricted." Do not allow battery optimization bypass.

Switch to iPhone

This entire report focuses on Android. On iOS, most of the described surveillance methods are not feasible. The following remains possible on iOS: geolocation (if permission was granted), contacts (if granted), camera/microphone (if granted), VPN detection via `utun` (partially), behavioral analytics via SDKs. But the volume of surveillance is significantly lower —of the 68 checks in the report, approximately 20–25 are feasible on iOS.Enabling Lockdown Mode on iPhone even further reduces this number.

Important caveat: iPhone does not share VPN through its hotspot. Unlike Android, where VPN can route hotspot traffic through the tunnel, iOS Personal Hotspot sends traffic from connected devices directly to the cellular network, bypassing the VPN. For VPN tethering, use an Android phone or a dedicated router.

Other

Clipboard: Wildberries intercepts it in the background. Use a password manager with autofill.

Part 2. You Have Left Russia

Threat model: Russian servers may infer your location based on IP address, GPS data, app list, contacts, SIM roaming status, and time zone.

Isolation Is Mandatory

If foreign apps are installed on the same device as Sberbank, any such app that sends a list of installed programs to a server reveals the user's country.

- **The best option is to have two phones**. Dedicate an old iPhone solely for Russian apps.
- **If you have only one phone**, you should use Work Profile (Shelter). This way, Russian apps cannot see the app list from the main profile.

It is advisable to keep a Russian VPN enabled on the phone used for Russian apps, since an open IP reveals your approximate geolocation. Additionally, your location leaks through: GPS, cell towers (Russian carrier via roaming), app list (local services), and device time zone. Each of these channels ideally be closed separately.

Geolocation

Revoke geolocation permissions from all Russian apps. For navigation abroad, use Google Maps or OsmAnd. If Yandex Go is required, grant location access only while the app is in use.

Contacts

It is better to revoke contact access from all Russian apps.

SIM Card

A Russian mobile carrier sees roaming when a user connects to its SIM card abroad. It should be switched to "SMS only" mode (e.g., for bank

confirmations). Ideally, the Russian SIM should be used in a separate phone for Russian apps, while the main (local foreign) SIM is used in the primary phone.

Update of April 16, 2026: Re-analysis of 30 popular Russian apps

Methodology

According to media reports, Russia's Ministry of Digital Development set April 15 as the expected date for introducing restrictions on users with VPN enabled. The restrictions are to be implemented by popular Russian online stores and internet services,including through their apps.

RKS Global researchers conducted a re-analysis of the same 30 apps that were examined earlier. Updated APK versions were obtained (26 out of 30 were updated between April 7 and April 16). The research method is static APK analysis (decompilation via apktool + jadx, native library analysis, decoding of XOR-obfuscated strings) plus dynamic on-device testing: Pixel 7a, Android 16, Magisk root, frida-server; VPN — AmneziaVPN (WireGuard, tun0 interface); each app launched for 15 seconds, adb logcat -d capture, VPN ON vs. VPN OFF comparison.

Key Findings

All 30 out of 30 apps detect VPN (in the first analysis it was 22 out of 30). 20 out of 30 actively block or restrict functionality upon VPN detection. Seven apps obtain the complete list of installed VPN clients. The number of detected VPN-detection methods grew from 6 to 10: in addition to the previous ones (hasTransport, interface scanning, /proc/net/tcp, proxy settings, Tor detection, server transmission), the following have been added: full-screen UI blocking, VPN app enumeration via queryIntentServices, a probabilistic model with weights, and MTU <1400 heuristics.

List of Installed VPN Clients

Seven apps — Wildberries, 2GIS, MTS, Ozon, MegaMarket, RuStore, Odnoklassniki — obtain a complete list of VPN clients through the system call queryIntentServices("android.net.VpnService"), which returns the names of all installed VPN apps (AmneziaVPN, WireGuard, OpenVPN, NordVPN, etc.).

In five of the seven, the list is transmitted via the BI.ZONE antifraud SDK together with 77 other device parameters. The manifest of each of the seven apps contains the block <queries><intent><action android:name="android.net.VpnService"/></intent></queries>.

Centralization of VPN Surveillance within Ecosystems

All seven Yandex apps (Browser, Maps, Market, Eda, Kinopoisk, Music, Go) use a single Yandex Passport SDK with CheckVpnStatusUseCase, a POST request to mobileproxy.passport.yandex.net/tmgrdfrend/checkvpn (with GPS, SIM card region, and device ID in the payload), and full-screen VpnChallengeActivity blocking on denial. The server flag android_block_vpn allows blocking to be enabled remotely in any of the seven apps; the VpnStatusChangedCommand mechanism provides IPC exchange of VPN status among them on the same device.

Mail.ru Mail (VpnProbabilityConnectivityChecker) and Dzen (the ru.zen.zapret module) have implemented an identical probabilistic model: five signals (hasTransport, interface scan, proxy, MTU <1400, and others) with two weight tables (cellular/WiFi) and four confidence levels. Sberbank, via the Kaspersky SDK, uses an 11-position enum com.kavsdk.internal.wifi.VpnClientStatus — from VpnClientUnavailable through installation, launch, active state, disconnection, to automatic reconnection.

Dynamic Testing

For Yandex Go, 77 logcat events were recorded over 15 seconds with VPN enabled vs. 39 without VPN; AppMetrica logs isVpn:true in every network event:

AppMetrica: [ru.yandex.taxi] Event received: Network.Proxy. With value: {networkType=wifi, isVpn=true, duration=0, url=https://mob-manager-aws.mob.taxi.yandex.net/, type=DIRECT}

For 2GIS, the logcat contains direct detection text and calls to a dedicated endpoint:

Grym/DeviceState: [VPN] Detected via TRANSPORT_VPN

Over 15 seconds — four requests to relay-api.eu.2gis.com/v1/vpn-detection-free. For Yandex Eda, with VPN enabled, the server returns checkVpnStatusUseCase Allowed false — the app blocks access.

VPN-Detection Obfuscation in MAX

In the MAX messenger (DPS SDK, package ru.trace_flow.dps), network interface names (tun, ppp, tap, pptp0) are encoded with the XOR key 0xDE60D9E8 and decoded at runtime. The SDK makes calls to six hardcoded IP-check endpoints (api.ipify.org, checkip.amazonaws.com, ifconfig.me, ip.mail.ru, ipv4/ipv6-internet.yandex.net) to compare the real IP with the VPN IP — the only such case among the 30 apps. There are four VPN-flag exfiltration channels: trace-flow.ru/api/v1/report, api.oneme.ru, vk-analytics.ru, apptracer.ru.

Adjustment of Recommendations

1. **Split tunneling** (which excludes Russian apps from the VPN tunnel, proposed in the first version as a partial solution) **is insufficient against the new detection methods.**

Thirteen apps scan network interfaces via the NetworkInterface.getNetworkInterfaces() — this API returns tun0 to any app regardless of routing, because Android does not isolate the network namespace per process. Seven apps use queryIntentServices to obtain the list of installed VPN clients — this method checks the PackageManager, not the network stack. Mail.ru and Dzen include an MTU <1400 heuristic in their probabilistic model, which triggers on tun0 regardless of whether the app is excluded from the tunnel. Two apps read /proc/net/tcp — a global kernel table accessible to all processes.

2. **VPN on a router remains effective**. When a phone connects to a router with VPN via Wi-Fi, no tun0 is created on the device, the MTU does not change, and no VPN transport is activated at the Android API level. All 10 detected detection methods operate at the device's network stack level — when tunneling is performed at the router level, they do not trigger.

3. **Android Work Profile (Shelter) changes from an "additional measure" to a critical measure due to VPN app enumeration.** If a VPN client is installed in the same profile as one of the seven apps that use queryIntentServices (Wildberries, Ozon, MTS, MegaMarket, RuStore, 2GIS, Odnoklassniki), they will obtain its package name and transmit it to the server via the antifraud SDK.

We thank the community for its interest in our work, its support, and its criticism of our ideas. We encourage the exchange of data and the development and expansion of our shared expertise. If you have questions or suggestions for the technical team, please write to tech@rks.global.