SORM
Le système de surveillance de masse russe depuis 1990

Stéphane FOSSE
fosse.fr

2 février 2026

SORM, acronyme russe de « Система оперативно-розыскных мероприятий » (Système de mesures opérationnelles d'enquête), constitue l'épine dorsale de la surveillance électronique en Russie depuis 1990. Conçu initialement par un institut de recherche du KGB au milieu des années 1980 pour intercepter les communications téléphoniques fixes, ce système s'est progressivement étendu aux réseaux mobiles, à Internet et aux réseaux sociaux. Son architecture repose sur un principe simple mais redoutable : des équipements d'interception installés directement chez les opérateurs télécoms et fournisseurs d'accès, connectés à des panneaux de contrôle dans les locaux du FSB, sans que les opérateurs n'aient connaissance des interceptions en cours.

Le modèle diffère radicalement des systèmes occidentaux d'interception légale. Aux États-Unis ou en Europe, les forces de l'ordre doivent présenter un mandat judiciaire aux opérateurs pour obtenir l'interception de communications spécifiques. En Russie, les agents du FSB obtiennent bien une autorisation judiciaire, mais ils n'ont aucune obligation de la montrer à quiconque en dehors de leur hiérarchie. Les opérateurs télécoms n'ont pas le droit de demander à voir le mandat. Ils n'ont pas accès aux équipements SORM installés dans leurs propres infrastructures. Ils ignorent qui est surveillé, quand et pourquoi.

1 De l'écoute téléphonique à la surveillance totale

Le projet SORM naît dans le laboratoire de recherche du KGB situé à Koutchino, dans la banlieue de Moscou, durant la seconde moitié des années 1980. La 12e Section du KGB supervisait alors les aspects techniques des écoutes téléphoniques sur les centraux analogiques. Après l'effondrement de l'Union soviétique en 1991, le Service fédéral de sécurité (FSB), principal héritier du KGB, récupère le programme et le place sous son propre 12e Centre.

L'évolution technologique des télécommunications contraint le système à s'adapter. SORM-1, déployé au début des années 1990, cible les communications téléphoniques fixes et mobiles. En 1998, face à la démocratisation du courrier électronique, les régulateurs russes des télécommunications proposent que tous les fournisseurs d'accès Internet installent à leurs frais des « boîtes noires » SORM permettant au FSB d'intercepter le trafic web. C'est la naissance de SORM-2, dédié à la surveillance d'Internet, y compris le trafic GPRS. Les publicités des fabricants d'équipements d'interception annoncent ensuite SORM-3, capable de collecter les informations de tous les médias de communication, offrant un stockage de trois ans et un accès à l'ensemble des données sur les abonnés, y compris les enregistrements et les localisations.

Le système SORM-3 représente un saut qualitatif. Il ne se contente plus d'intercepter les communications en temps réel. Il agrège les données issues de sources hétérogènes : SMS, MMS, publications sur les forums, blogs et réseaux sociaux. Ces données alimentent des bases indexées et interrogeables. L'organisation investigative russe Dossier Center rapporte que SORM permet de filtrer les données par numéro de mobile, IMEI du téléphone, géolocalisation, nom complet, raison sociale, adresse IP, adresse email, identifiant sur les messageries instantanées, et même par fragment d'adresse ou de numéro.

2 Une architecture technique sans garde-fou

L'architecture SORM repose sur trois composantes. Les équipements matériels et logiciels installés chez les opérateurs télécoms et fournisseurs d'accès Internet constituent la première couche. La seconde comprend les panneaux de contrôle installés dans les locaux des services de sécurité et de renseignement, permettant l'accès à distance aux données interceptées. La troisième correspond aux canaux de transmission de données qui relient ces deux éléments.

La loi russe impose l'installation d'équipements SORM dans tous les centres de données et à tous les points de communication du trafic Internet, y compris les moteurs de recherche, les sites d'hébergement, les plateformes de messagerie et les réseaux sociaux. Les opérateurs qui ne respectent pas ces exigences risquent des amendes, puis le retrait de leur licence d'exploitation. Pour obtenir une licence en premier lieu, l'installation de l'équipement SORM est un prérequis.

Le VAS Experts, l'un des fournisseurs de composants SORM, explique sur son site web que « la personne surveillée ne peut en aucune façon déterminer que cela se produit, tout comme le fournisseur d'accès ne sait pas qui le service spécial surveille ». Cette opacité structurelle rend la détection et le suivi des opérations SORM considérablement plus difficiles que pour des logiciels espions commerciaux comme Predator, qui peuvent être identifiés via des modifications d'infrastructure. Dans l'affaire Roman Zakharov contre Russie de décembre 2015, la Cour européenne des droits de l'homme a exprimé son inquiétude quant à l'absence de journaux d'activité de recherche via SORM, empêchant virtuellement toute enquête sur un usage non autorisé du système.

Les lois anti-terrorisme dites « lois Yarovaya », adoptées en 2016, ont durci les obligations. Les opérateurs télécoms et fournisseurs d'accès Internet doivent désormais conserver tout le contenu des communications (voix, texte, vidéo, images) pendant six mois, et les métadonnées (expéditeur, destinataire, horodatage, localisation) pendant trois ans maximum. Ces données doivent être mises à disposition des autorités sur demande. Les coûts de mise en conformité incombent exclusivement aux opérateurs. En 2020, le FSB a commencé à exiger un accès distant, illimité et automatique à toutes les données utilisateurs, avec déchiffrement automatique des communications.

3 Un marché dominé par des entreprises liées aux services de sécurité

Le marché russe des équipements SORM est relativement consolidé. Le groupe Citadel, enregistré en 2015, domine le secteur avec une part estimée entre 60 et 80% selon le Département d'État américain. En février 2023, les États-Unis ont imposé des sanctions à Citadel et à ses entités affiliées. Le conglomérat a absorbé plusieurs fabricants de composants SORM : Malvin Systems, MFI Soft, Osnova Lab, Signatek et TekhArgos. Anton Cherepennikov, fondateur de Citadel décédé en juillet 2023, entretenait des liens avec l'oligarque Alisher Ousmanov, proche du président Vladimir Poutine. D'anciens responsables du FSB et du ministère de l'Intérieur occupaient des postes de direction au sein du groupe.

Norsi-Trans, basé à Moscou, représente le second acteur avec 20 à 40% du marché russe en 2019. L'entreprise produit les solutions « Vitok » pour SORM-2 et « Yakhont » pour SORM-3. Son président, Alexandre Ivanov, fut vice-ministre des Communications chargé des communications par satellite et radio en Union soviétique de 1989 à 1992, avant de servir plusieurs années dans les forces armées russes. À la création de l'entreprise en 2007, Ivanov déclarait ne voir « rien de mal à utiliser les ressources administratives et les relations avec les agences fédérales », mentionnant explicitement le FSB.

Protei, issu de l'Institut de recherche industrielle de Léningrad rattaché au ministère soviétique des Communications, développe et vend du matériel et des logiciels SORM pour les réseaux « en Russie et à l'étranger ». L'entreprise revendique plus de 400 clients dans plus de 40 pays et commercialise un centre d'opérations SORM spécifiquement destiné aux pays de la Communauté des États indépendants (CEI).

4 L'exportation d'un modèle de surveillance

Le système SORM a essaimé bien au-delà des frontières russes. En Asie centrale, la Biélorussie, le Kazakhstan, le Kirghizistan et l'Ouzbékistan ont adopté des systèmes de surveillance basés sur SORM, avec des législations imposant aux opérateurs télécoms d'installer des équipements compatibles. En Amérique latine, Cuba et le Nicaragua utilisent des technologies SORM fournies par des entreprises russes.

En Biélorussie, le décret présidentiel n°129 signé par Alexandre Loukachenko en mars 2010 a imposé SORM dans le pays. Tous les opérateurs télécoms doivent installer du matériel compatible, et les réseaux existants doivent être mis à niveau. En avril 2012, l'opérateur public Beltelecom annonçait avoir installé SORM. Les exigences techniques développées par le ministère des Communications stipulent que les opérateurs sont responsables de limiter l'accès du personnel aux équipements SORM, et que ces équipements « doivent être conçus pour ne laisser aucune trace des recherches à distance dans les registres des opérateurs ».

Au Kazakhstan, le Comité de sécurité nationale a implémenté en 2017 des réglementations permettant l'accès en temps réel aux réseaux via SORM. L'opérateur suédois Tele2, qui opérait dans le pays de 2010 à 2019, indiquait dans son rapport de sortie qu'« il n'était pas possible pour Tele2 KZ de savoir à quelle fréquence le système SORM était utilisé et si le mandat requis avait été obtenu ». Le Conseil de sécurité nationale kazakh aurait choisi de ne pas utiliser certains composants SORM-3 de fabrication russe, préférant développer des équivalents nationaux en raison de portes dérobées suspectées.

À Cuba, Protei a participé à plusieurs éditions de la Foire internationale de La Havane (FIHAV) destinée à présenter les produits russes aux marchés cubain et latino-américain. En mars 2024, l'entreprise a signé un accord avec l'opérateur public cubain Movitel. ETECSA, le monopole public cubain des télécommunications, figure parmi les clients identifiés de Protei.

5 L'ampleur de la surveillance et ses zones d'ombre

Les statistiques officielles publiées par la Cour suprême de Russie révèlent un doublement du nombre d'interceptions téléphoniques et de messages électroniques en six ans : 265 937 en 2007, 539 864 en 2012. Ces chiffres n'incluent pas les écoutes de contre-espionnage visant les citoyens russes et les étrangers.

Le nombre total de personnes surveillées via SORM à travers le monde demeure impossible à établir. Le système ne laisse pas de trace côté opérateur. Aucune autorité indépendante n'audite son utilisation. Les pays importateurs n'ont aucune obligation de transparence. Les données collectées alimentent vraisemblablement des bases de renseignement, mais leur exploitation ultérieure, leur éventuelle revente ou leur partage avec des acteurs tiers restent dans l'ombre.

En décembre 2011, neuf conversations téléphoniques de Boris Nemtsov, ancien vice-Premier ministre devenu figure de l'opposition, ont été publiées sur le site pro-gouvernemental lifenews.ru. Nemtsov a demandé une enquête officielle. À ce jour, aucun coupable n'a été identifié ni poursuivi. En novembre 2012, la Cour suprême de Russie a confirmé le droit des autorités à surveiller l'opposition : espionner Maxim Petlin, un leader régional de l'opposition à Iekaterinbourg, était légal puisqu'il avait participé à des rassemblements incluant des appels contre l'extension des pouvoirs des services de sécurité russes. La Cour a jugé qu'il s'agissait de demandes d'« actions extrémistes » justifiant la surveillance.

La fourniture de matériel et logiciels SORM à des gouvernements étrangers par des entreprises russes, particulièrement celles liées aux services de sécurité, implique vraisemblablement un certain degré d'accès de Moscou à ces systèmes. En juin 2024, le Bureau de l'industrie et de la sécurité du département américain du Commerce a interdit à Kaspersky Lab de fournir des logiciels ou services aux États-Unis, citant la « capacité et l'intention de la Russie d'exploiter les entreprises russes pour collecter et instrumentaliser des informations sensibles ». Les facteurs retenus s'appliquent aux fournisseurs SORM : juridiction russe imposant la coopération avec les demandes d'information, accès aux données sensibles des clients, capacité d'installer des logiciels malveillants ou de retenir des mises à jour critiques.

6 Un programme toujours actif et en expansion

SORM reste pleinement opérationnel en 2025. Le programme n'a jamais été interrompu depuis son déploiement initial en 1990. Son périmètre s'est au contraire étendu à chaque génération technologique. Les principaux fournisseurs continuent de développer de nouvelles solutions et de participer à des salons professionnels en Afrique, en Amérique latine et au Moyen-Orient.

Roskomnadzor, l'agence russe de régulation des télécommunications, s'appuie désormais sur l'infrastructure SORM pour bloquer le trafic vers et depuis des milliers de sites et services occidentaux. Le projet russe de « souveraineté numérique » visant à isoler l'Internet russe du réseau mondial fonctionne en synergie avec SORM pour créer un écosystème informationnel largement autonome et plus facilement surveillable.

Pour les entreprises et voyageurs étrangers, la présence de systèmes SORM dans un pays signale une capacité gouvernementale d'intercepter les télécommunications et le trafic Internet sans notification aux opérateurs. Le Département d'État américain avertit que les voyageurs étrangers en Biélorussie, au Kazakhstan, en Ouzbékistan, à Cuba et au Nicaragua peuvent être placés sous surveillance, y compris de leurs téléphones et communications Internet. À l'approche des Jeux olympiques d'hiver de Sotchi en 2014, le Bureau de la sécurité diplomatique du Département d'État conseillait aux Américains de voyager avec des appareils « propres », de garder le Wi-Fi désactivé, de ne pas se connecter aux FAI locaux, de changer tous leurs mots de passe avant et après le voyage, de retirer la batterie de leur smartphone lorsqu'il n'est pas utilisé, et de jeter téléphone et carte SIM avant de rentrer.

Références

[1] Peter Bourgelais. Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia. Access Now, 2013.

[2] CSIS. Reference Note on Russian Communications Surveillance. Center for Strategic et International Studies, 2014.

[3] Insikt Group. Tracking Deployment of Russian Surveillance Technologies in Central Asia and Latin America. TA-RU-2025-0107. Recorded Future, jan. 2025.

[4] Andrei Soldatov et Irina Borogan. Russia's Surveillance State. In : *World Policy Journal* 30.3 (2013).

[5] Gavin Wilde. Can Russia's SORM Weather the Sanctions Storm? In : *Russian Analytical Digest* 298 (juill. 2023).