Verint Systems : anatomie d'un marchand de surveillance de masse

De Comverse Infosys à Cognyte, l'histoire d'un acteur central du marché mondial de l'espionnage commercial

Stéphane FOSSE

fosse.fr

25 février 2026

Résumé

Verint Systems, société fondée en 1994 en tant que filiale de Comverse Technology sous le nom Comverse Infosys, est devenue l'un des principaux fournisseurs mondiaux d'équipements de surveillance étatique. Ses « centres de surveillance » — outils d'interception de masse des communications téléphoniques et Internet — ont été déployés dans plus de 75 pays, dont des régimes documentés pour leurs violations des droits humains. En 2021, Amnesty International a établi que la filiale israélienne de Verint avait fourni des équipements d'écoute au gouvernement du Soudan du Sud, dont les services de renseignement pratiquent exécutions extrajudiciaires et détentions arbitraires.

Des enregistreurs de centres d'appels aux « monitoring centers » nationaux

L'histoire de Verint commence dans les années 1980 chez Comverse Technology, un groupe israélo-américain spécialisé dans les télécommunications. Sa division Comverse Infosys développe alors AudioDisk, un système d'enregistrement numérique destiné aux forces de l'ordre : là où les agences policières utilisaient des bobines de ruban magnétique, AudioDisk proposait un enregistrement direct sur disque, une recherche instantanée et la gestion simultanée de centaines de lignes surveillées. Le marché des écoutes légales — le *lawful interception* — était en train de se numériser, et Comverse s'y positionnait tôt.

Le tournant intervient en 1994 avec l'adoption du *Communications Assistance for Law Enforcement Act* (CALEA) aux États-Unis. Cette loi oblige les opérateurs téléphoniques à intégrer des équipements permettant les écoutes légales directement dans leur infrastructure réseau. Concrètement, cela signifie qu'il ne s'agit plus d'installer ponctuellement du matériel sur une ligne : les routeurs et commutateurs eux-mêmes doivent exposer une interface d'interception permanente. Comverse Infosys, avec ses produits Reliant et Star-Gate, dispose exactement de cette technologie. Elle décroche des contrats avec la DEA, le FBI et plusieurs grands opérateurs américains — AT&T et Verizon en tête.

C'est là que la situation devient intéressante d'un point de vue architectural. Comverse Infosys ne se contente pas de livrer du matériel : elle en assure la maintenance à distance. Des agents fédéraux américains rapportent dès la fin des années 1990 des anomalies récurrentes : des suspects sous surveillance semblent changer de comportement peu après la mise en place d'une écoute. En 2001, le journaliste Carl Cameron, de Fox News, consacre une série d'enquêtes en quatre parties à ces dysfonctionnements, citant des agents de la DEA, du FBI et du State Department qui évoquent une « porte dérobée » dans les logiciels de Comverse. Un document interne de la FCC daté de 1999 signalait déjà que « plusieurs agences gouvernementales ont exprimé de sérieuses préoccupations sur le fait que trop de personnels non autorisés peuvent accéder au système d'écoute. » Les enquêtes internes du FBI sur Comverse sont arrêtées avant que le matériel ne soit jamais testé pour détecter des fuites. Poursuivre cette piste, selon des agents cités par Cameron, équivaut à un « suicide professionnel »[9].

En février 2002, Comverse Infosys change de nom et devient Verint Systems, Inc., cotée au NASDAQ. La société se sépare partiellement de sa maison mère tout en conservant une relation capitalistique avec elle. Elle entre sur les marchés avec un portefeuille technique étendu et une présence dans au moins 16 pays.

Un catalogue industriel pour l'espionnage d'État

En 2013, le journaliste Ryan Gallagher publie dans Slate une enquête qui décrit précisément ce que vend Verint aux gouvernements[6]. Ce ne sont pas des outils ciblés : ce sont des infrastructures d'écoute

nationale. Le produit phare s'appelle Vantage. Sa documentation marketing parle d'une « interception de masse à l'échelle nationale » permettant « l'analyse et l'exposition des menaces à partir de milliards de communications ». L'architecture est conçue pour s'intégrer directement dans l'infrastructure télécoms d'un pays entier.

La gamme complète comprend des outils de reconnaissance vocale, des dispositifs portables d'interception mobile sur de larges zones géographiques, et des outils de *data mining* pour construire des profils comportementaux en temps réel. Entre 2006 et 2011, les ventes de solutions de renseignement communicationnel de Verint progressent de presque 70 %, passant de 108 à 182 millions de dollars par an. En 2012, le chiffre d'affaires consolidé dépasse 840 millions de dollars.

Contactée pour connaître sa politique vis-à-vis des lignes directrices américaines « Know Your Customer », Verint décline toute interview, estimant qu'elle « n'a pas tendance à chercher une couverture approfondie de ce domaine d'activité. »

SkyLock : traquer n'importe qui via le protocole SS7

En 2013, Verint lance SkyLock. Le principe repose sur une faille structurelle du protocole SS7, conçu en 1975 pour permettre aux opérateurs téléphoniques de se coordonner lors des appels internationaux. SS7 n'a jamais été conçu pour sécuriser l'identité des interlocuteurs : il suppose que seuls de grands opérateurs de confiance y ont accès[4].

SkyLock exploite ce protocole pour localiser n'importe quel téléphone mobile dans le monde à partir de son numéro ou de son identifiant IMSI. Le système interroge le réseau SS7 et retourne la position de l'appareil au niveau de l'antenne-relais à laquelle il est connecté. Verint peut ensuite coupler SkyLock à ses propres équipements IMSI-catchers physiques pour affiner la localisation.

Une brochure commerciale confidentielle de 24 pages, obtenue par le *Washington Post* en 2014, décrit SkyLock comme « une approche nouvelle et rentable pour obtenir des informations de localisation mondiale sur des cibles connues »[12]. Les captures d'écran du logiciel montrent des cibles géolocalisées au Mexique, au Nigeria, au Brésil, en République du Congo, aux Émirats arabes unis et au Zimbabwe.

Verint contourne les limitations topologiques du réseau SS7 en installant des « hubs SS7 locaux » chez des opérateurs partenaires dans différents pays. La brochure revendique un taux de succès de localisation d'au moins 70 %. Elle précise que Verint ne révèle pas la position des abonnés israéliens en Israël, ni celle des abonnés américains.

Eric King, directeur adjoint de Privacy International, résume l'enjeu : « N'importe quel dictateur disposant de l'argent nécessaire peut espionner n'importe qui dans le monde. C'est un problème énorme. »[8]

Le Soudan du Sud, le Pérou, Trinité-et-Tobago : la liste des régimes clients

En 2016, l'Associated Press révèle que le Pérou a acquis pour 22 millions de dollars un système Verint baptisé « Pisco » — capable de cibler 5 000 individus simultanément et d'enregistrer les communications de 300 personnes en temps réel, avec huit salles d'écoute installées sur une base militaire de Lima[2]. Des personnels israéliens de Verint sont dépêchés sur place pour former les opérateurs péruviens. Trinité-et-Tobago a vécu un scandale similaire : 53 personnes furent surveillées illégalement en 2009.

Le cas le plus circonstancié est celui du Soudan du Sud, établi par Amnesty International en 2021[1]. Verint Systems Ltd., filiale israélienne, a fourni des équipements d'interception des communications et des services de maintenance au gouvernement sud-soudanais entre mars 2015 et février 2017. Le gouvernement contraint l'opérateur téléphonique Vivacell à payer Verint — au moins 762 236 dollars — pour que le Service de sécurité nationale (NSS) ait un accès direct aux réseaux télécoms du pays.

Le NSS est documenté par l'ONU pour ses détentions sans jugement, ses disparitions forcées et ses exécutions extrajudiciaires. Selon CyberScoop[11], des conversations interceptées ont été utilisées comme preuves en justice — certains dossiers rejetés par des juges pour enregistrements illégaux. L'autocensure est généralisée : les militants refusent de parler de sujets sensibles par téléphone, préférant les rencontres physiques ou les applications de messagerie chiffrée.

Privacy International signale des ventes similaires en Ouzbékistan et au Kazakhstan. Haaretz cite l'Azerbaïdjan, où la technologie Verint aurait servi à surveiller des personnes LGBT, et l'Indonésie.

La scission Cognyte : changer de nom, continuer les affaires

En décembre 2019, Verint annonce sa séparation en deux entités. L'annonce est présentée comme une réorientation vers les solutions d'engagement client civiles. Mais la pression des actionnaires s'accumule depuis plusieurs années face à l'exposition réputationnelle liée aux ventes à des régimes autoritaires.

Le 1er février 2021, la scission est effective[7]. Verint Systems, enregistrée aux États-Unis, garde le nom et se concentre sur les logiciels d'expérience client. Cognyte Software Ltd., enregistrée en Israël, hérite de

l'intégralité des activités de renseignement et surveillance gouvernementale, et commence à coter au NASDAQ le 2 février 2021 sous le symbole CGNT — le jour même de la publication du rapport Amnesty sur le Soudan du Sud.

Un avocat israélien spécialisé dans les droits humains, cité par le Tor Project, qualifie les activités de Cognyte de « complicité dans des crimes contre l'humanité »[10]. Le fonds souverain norvégien retire ses investissements de Cognyte en 2023 après qu'une enquête de Meta a mis au jour des abus généralisés.

Ce que révèle le modèle Verint sur le marché de la surveillance commerciale

Verint illustre les mécanismes structurels qui permettent à des technologies d'interception légale de se retrouver entre les mains de gouvernements répressifs.

Le premier mécanisme est la normalisation juridique : CALEA, en 1994, a contraint les opérateurs américains à intégrer des capacités d'écoute dans leur infrastructure, créant un marché captif et une architecture d'interception permanente dans le cœur des réseaux.

Le deuxième mécanisme est l'opacité des licences d'exportation. Le régime israélien de contrôle des exportations s'avère non conforme aux standards internationaux, selon Amnesty International. Les lettres adressées au ministère israélien de la Défense n'ont pas reçu de réponse.

Le troisième mécanisme — peut-être le plus insidieux — est le *spin-off* défensif. Quand la réputation d'une entité est trop dégradée, on scinde l'entreprise. La partie « problématique » repart sous une nouvelle identité. Les technologies, les équipes, les clients et les contrats restent identiques.

Ce modèle, que l'on retrouve chez d'autres acteurs israéliens du secteur, soulève une question systémique : les certifications de conformité, les audits de sécurité et les engagements contractuels ont-ils une valeur réelle quand le même logiciel peut être rebaptisé et revendu à un gouvernement qui détient des journalistes ? La question dépasse Verint. Elle concerne l'ensemble du marché du *lawful interception*, qui opère dans l'ombre des législations nationales, avec une transparence quasiment nulle et une responsabilisation quasi inexistante.

Références

[1] Amnesty International. These Walls Have Ears: The Chilling Effect of Surveillance in South Sudan. Rapport d'enquête. Index : AFR 65/3577/2021. Fév. 2021.

[2] Associated Press. Israeli-American Company Verint Systems Selling Cheap Surveillance Tech To Governments. Enquête AP sur le cas du Pérou et de Trinité-et-Tobago. Août 2016.

[3] James Bamford. Shady Companies With Ties to Israel Wiretap the U.S. for the NSA. Documente le rôle de Verint dans les écoutes de Verizon pour la NSA et les liens avec l'Unité 8200 israélienne. Avr. 2012.

[4] Matthew Braga. Inside SS7, the Insecure Global Cell Network That's Used to Track Phones. Analyse technique du protocole SS7 et de son exploitation par SkyLock.

[5] Citizen Lab. Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles. Déc. 2020.

[6] Ryan Gallagher. Meet the American Company Helping Governments Spy on "Billions" of Communications. In : *Slate* (jan. 2013).

[7] Golan Hazani. Verint completes spin-off of its defense activities into new company Cognyte Software. In : *CTech / Calcalist* (fév. 2021).

[8] Infosec Institute. SS7 Protocol: How Hackers Might Find You.

[9] Christopher Ketcham. An Israeli Trojan Horse. In : *CounterPunch* (sept. 2008). Enquête sur les allégations de backdoor dans les systèmes CALEA de Comverse Infosys/Verint.

[10] Tor Project. Surveillance as a Service: The Global Impact of Israeli "Defense" Technologies on Privacy and Human Rights. 2023.

[11] Shannon Vavra. South Sudan worked with Israeli surveillance company to monitor citizens, Amnesty finds. In : *CyberScoop* (fév. 2021).

[12] Verint Systems. SkyLock Product Description 2013. Brochure commerciale confidentielle divulguée, Washington Post / DocumentCloud. 2013.