La loi FRA suédoise

Quand un État neutre légalise la surveillance de masse

Stéphane Fosse
fosse.fr

07 mars 2026

Copyleft : cette œuvre est libre, vous pouvez la copier, la diffuser et la modifier
selon les termes de la Licence Art Libre

Le 18 juin 2008, le Riksdag suédois adopte la loi SFS 2008 :717, communément appelée « loi FRA » (*FRA-lagen*). Ce texte autorise la Försvarets radioanstalt (FRA), l'agence nationale de renseignement sur les signaux, à intercepter en masse l'ensemble du trafic câblé — internet, téléphonie, courriels — traversant les frontières suédoises. Sans mandat individuel. Sans suspicion préalable. Avec une obligation légale pour tous les opérateurs de livrer ces données à des points de collecte contrôlés par l'État. C'est, au moment de son adoption, l'un des régimes de surveillance de masse les plus étendus d'Europe.

Qu'est-ce que la loi FRA suédoise de 2008 et comment fonctionne-t-elle techniquement ?

La loi FRA ne crée pas un programme de surveillance à partir de rien. Elle légalise et étend un dispositif qui existait déjà, mais dans un contexte technologique radicalement différent. La FRA, fondée en 1942, opérait jusqu'alors sur les signaux radio et hertziens. Or, depuis les années 1990, les communications ont massivement migré vers les câbles à fibre optique — un phénomène qui menaçait de rendre l'agence obsolète. Le gouvernement de Göran Persson avait d'ailleurs commandé en 2003 un rapport d'enquête (SOU 2003 :30) sur cette transition technologique, et un premier texte législatif avait été esquissé dès 2005 (Ds 2005 :30).

La loi adoptée en 2008 repose sur une mécanique architecturale simple mais redoutable. Elle crée une obligation légale pour tous les fournisseurs de services de communications électroniques de transférer, sous la contrainte et en toute confidentialité, l'intégralité du trafic câblé traversant les frontières suédoises vers des « points d'interaction » — des nœuds de collecte contrôlés par la FRA. Il ne s'agit pas de cibler des individus ou des organisations : c'est l'ensemble du flux qui est capturé, filtré ensuite à l'aide de sélecteurs définis par des mandats délivrés par le tribunal du renseignement défense (Försvarsunderrättelsedomstolen). Le texte de la loi liste huit finalités autorisant la collecte, parmi lesquelles les menaces militaires extérieures, le terrorisme transfrontalier, la prolifération des armes de destruction massive, les menaces sur les infrastructures critiques, et les activités de renseignement étrangères contre les intérêts suédois.

Ce qui rend ce dispositif particulièrement extensif, c'est la réalité technique d'internet. Une communication entre deux Suédois peut très bien transiter par des nœuds situés en Allemagne, au Danemark ou aux États-Unis, avant de revenir en Suède — et donc de croiser les frontières suédoises à l'aller comme au retour. Comme le souligne EDRi dès août 2008, l'ensemble de la population suédoise et une fraction significative des utilisateurs étrangers se retrouvent de facto sous la surveillance potentielle de la FRA, indépendamment de tout soupçon [11]. Mark Klamberg, doctorant en droit à l'université de Stockholm qui a contribué à l'analyse technique de la loi en 2009, a établi qu'un seul câble à fibre optique pouvait transporter 400 gigabits par seconde à l'époque — l'équivalent des communications de 200 000 utilisateurs simultanés, une capacité attendue à 1 600 000 utilisateurs dès 2011 avec les améliorations de la technologie optique. La loi ne fixe aucun plafond sur le nombre de câbles accessibles [10].

Comment la Suède, officiellement neutre, est-elle devenue un acteur central de la surveillance mondiale ?

Le paradoxe suédois est saisissant. Pendant plus de deux siècles, la Suède a cultivé une image de neutralité militaire. Pourtant, selon un document de la NSA daté de 2006 et rendu public par les révélations d'Edward Snowden, la Suède faisait secrètement partie de la coopération de renseignement UKUSA depuis 1954 — le

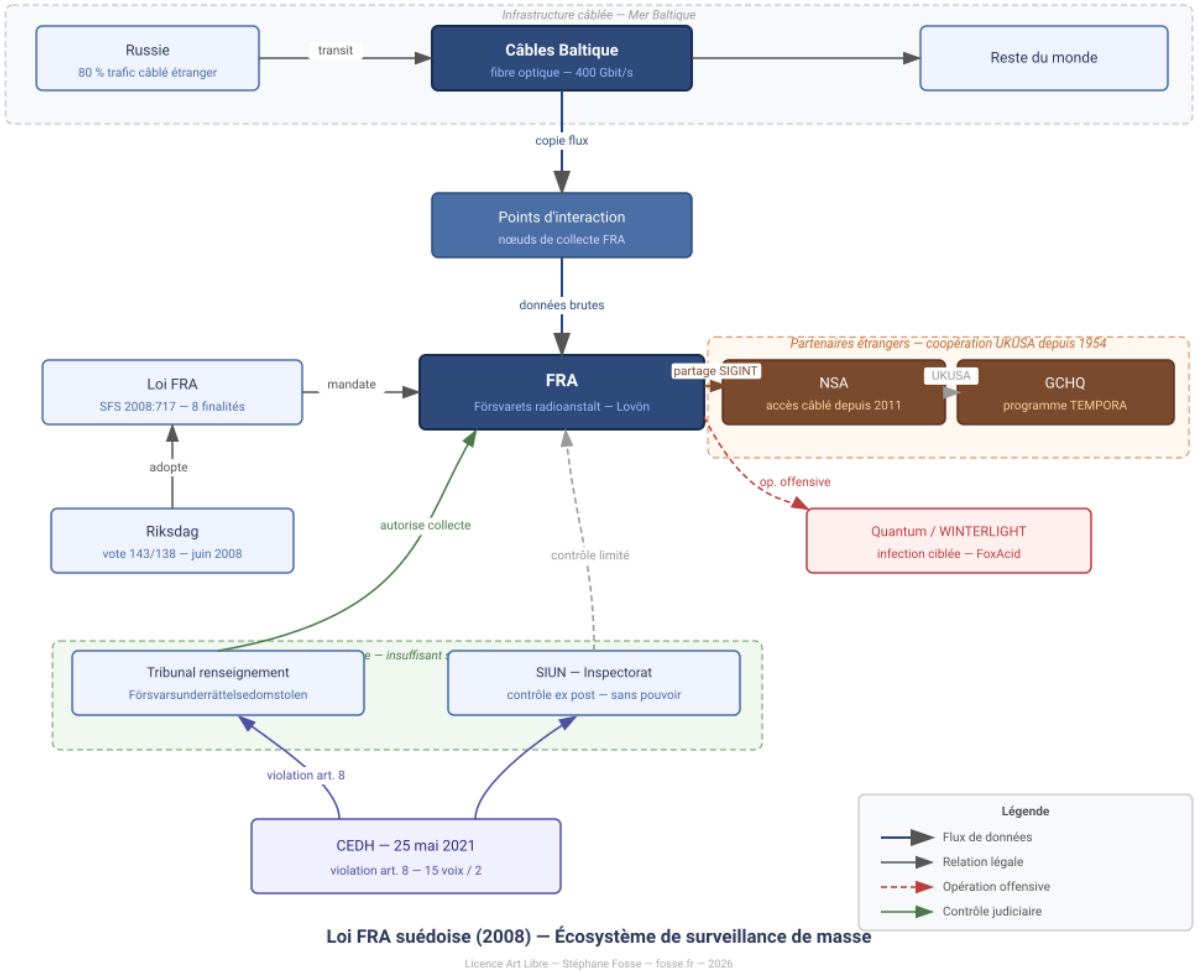

FIGURE 1 – Architecture technique du dispositif de collecte câblée de la FRA

même accord qui fonde les « Five Eyes » (États-Unis, Royaume-Uni, Canada, Australie, Nouvelle-Zélande). La NSA elle-même classifiait cette relation au niveau « top secret » précisément pour protéger l'image de neutralité politique de Stockholm [15].

La raison de cette valeur stratégique est géographique. Environ 80 % des communications câblées russes à destination de l'étranger transitent par les câbles sous-marins qui longent le fond de la mer Baltique et passent par la Suède. Le câble diplomatique de l'ambassade américaine à Stockholm, publié ultérieurement par WikiLeaks, l'écrivait noir sur blanc dès juillet 2008 : la loi FRA légalisait la surveillance de la majorité des communications transfrontalières russes. Wilhelm Agrell, professeur d'analyse du renseignement à l'université de Lund, résumait la situation à la presse suédoise en septembre 2013 : « La Suède est assise sur un pipeline rempli d'œufs en or » [17].

En 2004 — plusieurs années avant que le Riksdag ne vote la loi FRA — la NSA, le GCHQ et la FRA avaient d'ores et déjà signé un accord bilatéral permettant à la NSA de collaborer directement avec la FRA sans passer par l'intermédiaire britannique. Puis, en 2011, la FRA a accordé à la NSA un accès à sa collecte câblée. Le 24 avril 2013, six semaines avant les premières révélations Snowden, le général Keith Alexander, directeur de la NSA, recevait à Fort Meade une délégation suédoise conduite par Ingvar Åkesson, directeur de la FRA, accompagné de cinq membres de son état-major — une réunion de trois jours pour discuter, notamment, de l'élargissement de la coopération. Les documents Snowden révélés par la chaîne publique suédoise SVT en décembre 2013 confirmaient que la NSA considérait la FRA comme son partenaire principal pour le renseignement sur la Russie, qualifiant ses apports d'« uniques » et irremplaçables [16].

La collaboration dépassait la simple interception passive. La FRA participait au programme offensif Quantum, et plus précisément à l'opération WINTERLIGHT — un dispositif consistant à infecter les ordinateurs de cibles prioritaires avec des logiciels espions, en les redirigeant à leur insu vers des serveurs d'attaque baptisés « FoxAcid ». En mars 2013, la FRA rapportait à la NSA que l'opération avait généré 100 tentatives d'infection, dont cinq avaient été transmises aux serveurs du GCHQ. L'objectif affiché de la NSA était explicite dans ses documents internes : privilégier une relation bilatérale avec la FRA plutôt qu'un accord trilatéral incluant le GCHQ, dont la participation risquait d'être compromise par les contraintes légales britanniques [6]. L'enquête de Hugh Eakin publiée dans la *New York Review of Books* en 2017 résumait la situation : la Suède n'était pas une victime de la surveillance américaine, mais un acteur à part entière — peut-être le troisième plus important partenaire occidental, après les États-Unis et le Royaume-Uni.

Pourquoi la loi FRA a-t-elle été adoptée dans la controverse ?

Le vote du 18 juin 2008 a été l'un des plus tendus de l'histoire parlementaire suédoise récente. Le texte est passé à 143 voix contre 138, avec une abstention et 67 absents — soit une majorité d'un seul vote si l'on raisonne en termes de majorité effective. La veille du vote, alors que plusieurs parlementaires de la coalition de centre-droit semblaient sur le point de faire défection, le ministre de la Défense Sten Tolgfors avait conclu un accord de dernière minute avec Fredrick Federley, un député critique du Parti du Centre, promettant des protections supplémentaires pour la vie privée à une date ultérieure. Un seul parlementaire tint finalement ses engagements jusqu'au bout : Camilla Lindberg, du Parti libéral, qui vota contre son propre groupe [11].

La contestation ne venait pas uniquement des partis d'opposition. Parmi les institutions consultées lors de la procédure législative, huit avaient rendu des avis sévères : l'une qualifiait le texte d'« écoute sans mandat judiciaire », une autre de « surveillance générale du contenu des appels téléphoniques et messages », une troisième de « fondamentalement défaillant ». L'ancien directeur de la FRA lui-même avait déclaré que le dispositif était contraire au droit européen. L'agence de douanes suédoise, le Conseil d'inspection des données et les cours d'appel des régions de Skåne et Blekinge avaient également exprimé des réserves formelles. En dehors des frontières suédoises, la Finlande avait protesté diplomatiquement, et la Belgique avait envisagé de porter la Suède devant la Cour de Strasbourg — car une proportion importante du trafic internet norvégien et finlandais transitait également par les câbles suédois [7].

Le mandat de la FRA posait un problème de fond : il était formulé de façon extrêmement large. La loi l'autorisait à surveiller les « menaces extérieures » — une catégorie englobant les menaces militaires, le terrorisme, la sécurité informatique, les pénuries d'approvisionnement, les déséquilibres écologiques, les conflits ethniques et religieux, les migrations et les turbulences économiques comme la spéculation sur les monnaies. Surtout, contrairement à ce qu'affirmait le gouvernement, aucune suspicion individuelle n'était requise avant que la FRA ne procède à la surveillance d'un citoyen suédois. Le gouvernement prétendait que la FRA surveillait des « phénomènes » et non des individus — une distinction que les critiques, dont Klamberg, qualifiaient de « doublepensée » : surveiller des phénomènes sans surveiller les individus qui en sont les vecteurs était, techniquement, impossible.

Quelles sont les lacunes structurelles du régime de surveillance instauré par la loi FRA ?

La loi de 2008 a été amendée une première fois en décembre 2009 (suite à un accord politique conclu en septembre 2008), puis à trois reprises entre 2013 et 2016. Ces révisions ont introduit un tribunal du renseignement défense chargé d'autoriser préalablement toute opération de collecte, un Inspectorat du renseignement défense chargé du contrôle ex post, et un conseil interne de protection de la vie privée au sein de la FRA. La façade institutionnelle est solide. Les lacunes sont dans les détails.

Première lacune : l'absence de plafond sur le volume de collecte. La loi ne fixe aucune limite au nombre de câbles à fibre optique auxquels la FRA peut accéder — elle se borne à exiger que cet accès corresponde aux « besoins » de l'agence, sans définir ce terme ni imposer une évaluation de proportionnalité cumulée. La FRA peut donc accéder à un câble supplémentaire sans avoir à démontrer que les câbles déjà accessibles sont insuffisants [10].

Deuxième lacune : la dualité des activités « opérationnelles » et « de développement ». La loi crée, parallèlement aux huit finalités officielles, une catégorie distincte d'activités de « développement » destinées à surveiller l'environnement des signaux et les évolutions techniques. Ces activités de développement, décrites par le juge Pinto de Albuquerque de la CEDH comme un « véritable trou noir juridique », permettent la collecte et la conservation de grandes quantités de métadonnées, avec la possibilité légale de transférer ces données collectées dans le cadre des « activités de développement » vers les « activités de renseignement ». Cette passerelle contourne dans les faits les huit finalités encadrées.

Troisième lacune, peut-être la plus grave : le contrôle du partage international. Ni le gouvernement ni la FRA ne sont légalement obligés de tenir compte des intérêts individuels en matière de vie privée lorsqu'ils décident de transmettre des données interceptées à des gouvernements étrangers ou à des organisations internationales. Les données non personnelles — c'est-à-dire tout ce qui a été anonymisé ou traité de façon à ne plus contenir d'éléments d'identification directe — peuvent être conservées indéfiniment, transférées à des partenaires étrangers sans conditions, et utilisées à des fins incompatibles avec l'objet initial de la collecte [2].

L'Inspectorat du renseignement défense (SIUN), chargé du contrôle externe, ne peut que soumettre des remarques à la FRA ou en référer au gouvernement. Il n'a aucun pouvoir d'injonction contraignante, même en cas de violation avérée de la Constitution suédoise. Après les révélations Snowden de 2013, le rapport annuel du SIUN pour cette année-là ne mentionnait la coopération internationale de la FRA qu'en deux phrases, sans aucune allusion aux documents publiés. Le Parlement suédois avait conclu, sur la base de ce rapport, que « le système de protection de la vie privée fonctionne comme le législateur l'a voulu » [8].

Que dit l'arrêt de la Cour européenne des droits de l'homme du 25 mai 2021 ?

Le recours devant la CEDH avait été déposé dès le 14 juillet 2008 par Centrum för rättvisa, une fondation suédoise d'intérêt public spécialisée dans le contentieux des droits fondamentaux contre l'État. L'affaire traverse d'abord une chambre de troisième section, qui rend le 19 juin 2018 un arrêt unanime concluant à l'absence de violation de l'article 8 — tout en notant que la loi donnait « quelques raisons de s'inquiéter » quant aux risques d'abus. Centrum för rättvisa demande le renvoi en Grande Chambre. Il est accepté en février 2019, et une audience se tient le 10 juillet 2019 à Strasbourg.

Le 25 mai 2021, la Grande Chambre rend son arrêt par 15 voix contre 2 [4]. Elle reconnaît d'abord que la décision d'opérer un régime d'interception en masse ne viole pas en soi l'article 8 — les États disposent d'une large marge d'appréciation face à la prolifération des menaces de sécurité. Mais elle identifie trois déficiences structurelles spécifiques au régime suédois. La première : aucune règle claire n'impose la destruction du matériel intercepté ne contenant pas de données personnelles. La deuxième : aucune obligation légale ne contraint à tenir compte des intérêts individuels en matière de vie privée lors de la décision de transmettre des renseignements à des partenaires étrangers. La troisième : l'absence d'un contrôle ex post facto effectif — le contrôle a posteriori exercé par l'Inspectorat du renseignement défense étant trop limité dans ses pouvoirs pour constituer une garantie réelle.

Ces trois lacunes combinées font que le régime ne satisfait pas au critère de « garanties de bout en bout » (*end-to-end safeguards*) que la Cour définit pour les systèmes d'interception en masse. La Suède a été condamnée à verser 52 625 euros à Centrum för rättvisa en frais de procédure. L'arrêt, rendu le même jour que *Big Brother Watch v. United Kingdom* — qui concluait également à une violation de l'article 8 pour le programme TEMPORA du GCHQ — constitue un double précédent majeur pour le droit européen de la surveillance de masse.

La suite a pourtant déçu les défenseurs de la vie privée. Comme l'analyse Dataskydd.net pour EDRi en octobre 2021, les amendements proposés par le gouvernement suédois en réponse à l'arrêt n'ont pas corrigé les défauts identifiés : ils les ont aggravés. Le projet élargissait les cas autorisant la collecte en masse, et facilitait le

partage avec des partenaires étrangers en ajoutant une neuvième finalité — la « coopération internationale » — non reliée à une menace contre les intérêts suédois [5].

Conclusion : la neutralité comme paravent

La loi FRA de 2008 illustre une tension que les architectes des systèmes numériques connaissent bien : la discordance entre ce qu'un système est présenté comme faisant et ce qu'il fait effectivement. La Suède se présentait comme neutre et défenseure de la liberté sur internet dans les pays en développement — tout en opérant l'un des régimes de surveillance câblée les plus étendus d'Europe, en partenariat secret avec la NSA depuis 1954. La loi FRA n'est pas un accident ou une dérive : c'est l'aboutissement d'une stratégie délibérée de repositionnement d'une agence de renseignement face à la migration des communications vers les câbles à fibre optique, conduite avec l'appui actif de partenaires américains et britanniques.

Ce que Snowden avait dit en mars 2014 devant le Parlement européen mérite d'être retenu : entre la FRA et la NSA, la différence n'est pas de nature mais d'échelle — budget et effectifs. La loi FRA a fourni une couverture légale à un programme de collecte qui existait avant elle, et a étendu ses capacités à un moment précis où la NSA cherchait elle-même à consolider ses partenariats câblés, dans un contexte où les contraintes légales britanniques rendaient le GCHQ moins fiable. La coïncidence de calendrier avec les amendements au Foreign Intelligence Surveillance Act américain, effectifs en juillet 2008, n'est pas anodine.

Pour les citoyens suédois comme pour les millions d'autres dont les communications transitent par la Baltique, la vraie question posée par la loi FRA n'est pas celle de son existence — les États conduisent du renseignement, c'est une réalité — mais celle de ses garde-fous. L'arrêt de la CEDH de 2021 l'a dit clairement : des garanties juridiques formelles ne valent que si elles sont applicables, indépendantes, et dotées de pouvoirs effectifs. Un tribunal qui siège en secret, dont les décisions sont définitives et non susceptibles d'appel, qui ne peut être saisi que par l'agence qu'il est censé contrôler — n'est pas un contrôle. C'est un ornement.

La FRA opère aujourd'hui sur deux axes principaux : le renseignement sur les signaux (SIGINT) à destination du gouvernement et des forces armées, et la cybersécurité pour les infrastructures critiques. Son siège est à Lovön, à l'ouest de Stockholm. Quelques faits récents :

- Le budget de la FRA est passé de 1,582 milliard de couronnes suédoises en 2022 à 1,927 milliard en 2023, puis 2,295 milliards en 2024 et 2,785 milliards en 2025 — une quasi-doublement en trois ans, justifié officiellement par la « détérioration de la situation sécuritaire » dans l'environnement proche de la Suède ;
- Depuis le 1er novembre 2024, la FRA a repris la direction du Centre national de cybersécurité (NCSC), avec 50 millions de couronnes supplémentaires alloués par le gouvernement pour développer ce centre ;
- La FRA a publié son rapport annuel 2024 sous le titre « Utmanande och komplex hotbild » (« Menaces complexes et difficiles »), indiquant que la demande de renseignements et de services de cybersécurité continue d'augmenter ;
- En mars 2024, le drapeau de l'OTAN a été hissé devant le siège de la FRA à Lovön X — symbole de l'intégration de la Suède dans l'alliance atlantique après son adhésion officielle le 7 mars 2024. Ce changement de statut renforce encore la légitimité institutionnelle de la FRA dans la coopération de renseignement occidentale.

la FRA n'a jamais été aussi bien dotée, aussi légitime officiellement, et aussi centrale dans le dispositif de sécurité suédois. Le contexte — guerre en Ukraine depuis 2022, adhésion à l'OTAN en 2024, menaces cyber russes documentées — lui fournit un environnement politique particulièrement favorable. Si l'arrêt CEDH de 2021 a formellement contraint la Suède à amender sa législation, les amendments adoptés ont, comme l'analysait EDRi, élargi les capacités plutôt que de les restreindre. La FRA de 2026 est une agence plus grande, mieux financée et dotée d'un mandat plus large qu'en 2008.

Références

[1] Agence des droits fondamentaux de l'Union européenne. National intelligence authorities and surveillance in Sweden — Short Thematic Report. Anglais. 2014.

[2] Centrum för rättvisa. FRAgile liberty: why we brought Sweden before the Strasbourg court. Anglais. about:intel, 2019.

[3] Civil Rights Defenders. The UN Reviews Swedish Signals Intelligence and Privacy. Anglais. Mars 2016.

[4] Cour européenne des droits de l'homme, Grande Chambre. Centrum för rättvisa c. Suède. Arrêt du 25 mai 2021. Violation de l'article 8 de la Convention européenne des droits de l'homme. 2021.

[5] Dataskydd.net. The terrifying expansion of Sweden's state surveillance. Anglais. European Digital Rights (EDRi), oct. 2021.

[6] Hugh Eakin. The Swedish Kings of Cyberwar. Anglais. In : *New York Review of Books* (jan. 2017).

[7] European Digital Rights (EDRi). Norwegian group joins Sweden-based Justice Center against Swedish FRA law. Anglais. 2009.

[8] Ezouave. Sweden. Anglais. Mai 2015.

[9] Greffe de la Cour européenne des droits de l'homme. Insufficient safeguards in bulk signals-intelligence gathering risked arbitrariness and abuse — ECHR 164 (2021). Anglais. 2021.

[10] Mark Klamberg. Big Brother's Little, More Dangerous Brother. Anglais. Verfassungsblog, 2021.

[11] Mark Klamberg. ENDitorial: Wiretapping — the Swedish way. Anglais. European Digital Rights (EDRi), août 2008.

[12] Law Library of Congress. Foreign Intelligence Gathering Laws: Sweden. Anglais. 2014.

[13] Asaf Lubin. Legitimizing Foreign Mass Surveillance in the European Court of Human Rights. Anglais. Just Security, 2018.

[14] Riksdag suédois. Lag om signalspaning i försvarsunderrättelseverksamhet. Suédois. Adoptée le 18 juin 2008, entrée en vigueur le 1er janvier 2009. 2008.

[15] SVT Nyheter. Read the Snowden Documents From the NSA. Anglais. Déc. 2013.

[16] SVT Nyheter / Uppdrag granskning. Snowden files reveal Swedish-American surveillance of Russia. Anglais. Déc. 2013.

[17] The Local / TT. Sweden sits on pipeline of intelligence 'gold'. Anglais. Sept. 2013.