ORGANISATION SUISSE D'AIDE AUX RÉFUGIÉS
www.osar.ch

Iran: surveillance des réseaux sociaux à l'étranger

Papier thématique de l'analyse-pays de l'OSAR

Berne, le 25 novembre 2023

Mentions légales

Editeur

Organisation suisse d'aide aux réfugiés (OSAR)
Case postale, 3001 Berne
Tél. 031 370 75 75
Courriel : info@osar.ch
Site web : www.osar.ch
IBAN : CH92 0900 0000 3000 1085 7

Version disponible en allemand et français.

Sommaire

Ce rapport repose sur des renseignements d'expert·e·s et sur les propres recherches de l'Organisation suisse d'aide aux réfugiés (OSAR). Conformément aux standards COI, l'OSAR fonde ses recherches sur des sources accessibles publiquement. Lorsque les informations obtenues dans le temps imparti sont insuffisantes, elle fait appel à des expert·e·s. L'OSAR documente ses sources de manière transparente et traçable, mais peut toutefois décider de les anonymiser, afin de garantir la protection de ses contacts.

1 Introduction

Les questions suivantes sont tirées d'une demande adressée à l'analyse-pays de l'OSAR.

1. Les propos tenus par les ressortissant·e·s iranien·ne·s sur les réseaux sociaux (Facebook, Instagram, Twitter, Telegram, etc.) sont-ils surveillés (toujours/régulièrement/au cas par cas) ? Dispose-t-on d'informations permettant de savoir si une distinction est faite pour d'éventuelles mesures répressives de l'État,

    a. en fonction de la portée de l'activité ou de la déclaration (par exemple combien de personnes l'ont immédiatement vue/entendue, l'activité ou la déclaration a-t-elle été faite dans un média public, combien de *followers* suivent l'activité sur les réseaux sociaux) ?

    b. s'il s'agit de propos tenus directement par une personne ou, par exemple, de propos/contenus/caricatures de tiers simplement partagés ou relayés sur les réseaux sociaux ?

L'analyse-pays de l'OSAR observe les développements en Iran depuis plusieurs années.[1] Sur la base de ses propres recherches ainsi que de renseignements transmis par des expert·e·s externes, elle apporte les réponses suivantes aux questions ci-dessus.

2 Surveillance des réseaux sociaux

L'Iran a obtenu des technologies de surveillance avancées provenant d'autres États. D'après les indications de *Freedom House*, l'Iran a acquis des technologies de surveillance auprès d'autres gouvernements autoritaires, dont la Chine et la Russie. En mars 2023, le *Wall Street Journal* a rapporté que le gouvernement russe avait vendu à l'Iran des technologies incluant des logiciels de « surveillance des communications »[2].

Surveillance massive des activités sur les réseaux sociaux en Iran. Selon *Freedom House*, la sphère en ligne en Iran est fortement surveillée par l'État iranien. Des enquêtes publiées en 2022 par *Intercept* et *Citizen Lab* ont révélé que les autorités gouvernementales ont la capacité d'intercepter, de stocker et d'analyser en masse les données des téléphones portables des utilisatrices et utilisateurs à des fins de surveillance. L'État iranien surveille les réseaux sociaux pour détecter les activités qu'il considère comme illégales. Des outils de *Deep Packet Inspection*[3] permettent aux autorités de filtrer les contenus en ligne et d'analyser simultanément l'historique de navigation et les communications. Selon *Freedom House*, des

1 https://www.osar.ch/publications/rapports-sur-les-pays-dorigine.
2 Freedom House, Freedom on the Net 2023 - Iran, 4 octobre 2023: https://freedomhouse.org/country/iran/freedom-net/2023.
3 La Deep Packet Inspection est une méthode élaborée d'analyse, de surveillance, de filtrage et de marquage des paquets de données transmis sur un réseau. Dans certains États, la DPI est utilisée afin de surveiller le trafic Internet des citoyen·ne·s ou pour censurer du contenu. Security Insider, Was ist Deep Packet Inspection (DPI)? 23 juin 2021: https://www.security-insider.de/was-ist-deep-packet-inspection-dpi-a-1052442/.

représentant·e·s des autorités avaient admis par le passé avoir surveillé les publications en ligne d'activistes et de manifestant·e·s[4].

Surveillance des applications domestiques de communication et de réseaux sociaux. Au cours des dernières années, selon *Freedom House*, les autorités ont promu des applications de communication et de réseaux sociaux domestiques, dont les liens avec les services de renseignement iraniens ont été révélés[5]. Diverses sources estiment que l'utilisation d'applications de messagerie domestiques permet une surveillance des autorités[6]. En mars 2002, le ministre des TIC a annoncé que les forces de sécurité devraient être autorisées à accéder aux données des utilisatrices et utilisateurs de ces applications avec un mandat de perquisition. D'après le *New Lines Magazine*, les dirigeants de Rubika, l'une des applications de messagerie domestiques iraniennes, ont affirmé utiliser l'intelligence artificielle (IA) pour identifier et supprimer de l'application les contenus perçus comme « immoraux »[7]. Selon la *personne de contact H*,[8] les membres de la diaspora qui utilisent ces applications iraniennes constituent des « cibles faciles » pour les autorités et font l'objet de surveillance[9].

Pas de « preuve solide » d'une surveillance de masse automatisée. La surveillance des réseaux sociaux consiste souvent à essayer de dérober les mots de passe des personnes par différents moyens, à surveiller l'activité sur les réseaux sociaux ouverts et à créer des faux comptes dans des groupes sur Internet et sur les réseaux sociaux. La *personne de contact I*[10] n'est pas convaincu que les autorités iraniennes puissent procéder à une surveillance de masse automatisée des réseaux sociaux. Il estime néanmoins que le niveau de surveillance de la masse est très élevé. Cela accroît le sentiment d'arbitraire et d'imprévisibilité[11]. Selon la *personne de contact H*, la surveillance numérique serait en quelque sorte systématique, sans toutefois être comparable à l'approche adoptée en Russie et en Chine. La *personne de contact H* relève que les autorités iraniennes ont obtenu une technologie de surveillance russe. Il est évident que les autorités collectent des données, mais il n'existerait pas de « preuve concrète » de l'utilisation de cette technologie à des fins de surveillance de masse automatisée[12]. La *personne de contact G*[13] a souligné que les autorités iraniennes n'avaient pas la capacité de surveiller l'ensemble des utilisatrices et utilisateurs des réseaux sociaux, faute de ressources suffisantes[14]. *Article 19* informait en novembre 2019 que les services secrets iraniens tentent de donner l'impression qu'ils arrivent astucieusement à surveiller Internet et les réseaux sociaux. En pratique, la surveillance des réseaux sociaux consiste souvent à tenter de soutirer les mots de passe des personnes de différentes

4 Freedom House, Freedom on the Net 2023 - Iran, 4 octobre 2023.
5 Ibid.
6 Ibid.; entretien téléphonique du 27 octobre 2023 avec la personne de contact H.
7 Freedom House, Freedom on the Net 2023 - Iran, 4 octobre 2023.
8 La personne de contact H est une personne experte en cybersécurité et spécialiste de l'Iran.
9 Entretien téléphonique du 27 octobre 2023 avec la personne de contact H.
10 La personne de contact I dispose de connaissances spécialisées en matière de répression transnationale et de surveillance numérique par l'État iranien.
11 Entretien téléphonique du 15 septembre 2023 avec la personne de contact I.
12 Entretien téléphonique du 27 octobre 2023 avec la personne de contact H.
13 La personne de contact G est une personne dont l'expertise est reconnue en matière de censure internet iranienne, de cyberattaques et de sécurité numérique.
14 Entretien téléphonique du 23 octobre 2023 avec la personne de contact G.

façons, à surveiller l'activité sur les réseaux sociaux ouverts et à créer des faux comptes dans des groupes en ligne et sur les réseaux sociaux[15].

Les capacités de renseignement de l'Iran reposent sur un grand nombre de personnes qui collectent en sa faveur des informations sur les activités en ligne. Selon l'organisation américaine *Atlantic Council*, les capacités des services de renseignement de l'Iran ne reposent pas en premier lieu sur une technologie de pointe, mais plutôt sur le grand nombre de personnes qui travaillent pour eux et partagent des informations sur ce qu'elles observent en ligne[16]. La *personne de contact H* relève que les services de renseignement iraniens disposent actuellement de nombreux collaborateurs·trices qui collectent des informations pour leur compte[17]. La *personne de contact I* a également souligné que les propos tenus par des membres du gouvernement iranien permettaient de conclure qu'il y avait suffisamment de personnel pour collecter amplement des informations et réagir aux messages critiques à l'égard du gouvernement sur les réseaux sociaux. Selon la *personne de contact I*, il est difficile d'évaluer le degré réel de coordination et le mode d'exploitation par le service de renseignement[18].

Des rapports ont démontré que les autorités de sécurité iraniennes analysaient systématiquement et de manière détaillée des sujets spécifiques dans les réseaux sociaux. La *personne de contact G* indique que les services de sécurité iraniens peuvent mettre en place une équipe spécialisée lorsqu'ils s'intéressent à une thématique particulière sur les réseaux sociaux. Cette équipe enquêterait alors sur le sujet de manière systématique[19]. Il ressort de certains courriels piratés des autorités iraniennes analysés par *Miaan Group* que les autorités iraniennes ont mandaté *LifeWeb*, un groupe iranien d'analyse des réseaux sociaux. Ce dernier a été engagé pour analyser les réactions des utilisatrices et utilisateurs iranien·ne·s sur Twitter, Instagram et Telegram suite à l'abattage d'un avion ukrainien au-dessus de Téhéran en janvier 2020. *LifeWeb* avait alors rédigé un rapport très complet sur ce sujet pour les services de sécurité iraniens. Ce faisant, *LifeWeb* avait dépassé le cadre de l'analyse stricto sensu des réseaux sociaux pour s'occuper également de l'analyse du contenu politique[20].

---

15 Commissariat général aux réfugiés et aux apatrides (Belgique), département de recherche COI (CGRA-CEDOCA), Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10 mai 2023, p. 20: https://www.ecoi.net/en/file/local/2092670/coi_focus_iran._surveillance_van_de_diaspora_door_de_iraanse_autoriteiten_20230510.pdf.

16 Ibid.

17 Entretien téléphonique du 27 octobre 2023 avec la personne de contact H.

18 Entretien téléphonique du 15 septembre 2023 avec la personne de contact I.

19 Entretien téléphonique du 23 octobre 2023 avec la personne de contact G.

20 Ibid.; Miaan Group, Internet Oppressors: A Look at the Office of Iran's Attorney General and its Contractors, Unveiling the Involvement of Private Companies, Academic Institutions, Judicial Bodies, and Security Organizations in Iran's Internet Repression, juillet 2023, p. 44: https://filter.watch/en/wp-content/uploads/sites/2/2023/09/Internet-Oppressors-Report-2023.pdf.

Ingénierie sociale et découverte de réseaux. La surveillance s'effectue souvent au moyen de logiciels malveillants, tels que des *malwares*[21], et d'attaques par hameçonnage (*phishing*)[22], conçus pour inciter les destinataires à partager des données sensibles[23]. Il ressort des conclusions actuelles du *Bundesamt für Verfassungsschutz* (Office fédéral allemand de protection de la Constitution, ci-après : BfV) que le groupe *Charming Kitten* tente concrètement d'espionner des personnes et des organisations iraniennes en Allemagne. À cet effet, le groupe applique des méthodes sophistiquées d'ingénierie sociale et développe des identités en ligne sur mesure en fonction des victimes[24]. L'ingénierie sociale (*Social Engineering*) consiste ici à préparer une cyberattaque et mettre au point un récit qui incite la victime à entreprendre une certaine action, par exemple ouvrir une pièce jointe dans un courriel contenant un programme malveillant[25]. La *personne de contact G* a déclaré que les services secrets iraniens sont capables de mener des recherches OSINT (*Open Source Intelligence*) exigeantes et de très bonne qualité. Dans un cas rapporté par le *Miaan Group*, un groupe de pirates informatiques du gouvernement iranien a obtenu une grande quantité d'informations sur une figure de l'opposition politique à l'étranger. Ceux-ci ont mené des recherches approfondies et sophistiquées sur cette personne. Ayant découvert qu'elle souhaitait solliciter un permis de conduire, les hackers ont alors créé un formulaire de demande de permis de conduire gratuit pour la personne à l'étranger comme technique d'hameçonnage[26]. Selon l'*expert en cybersécurité X*, l'objectif principal des activités de surveillance des autorités iraniennes à l'étranger est d'élaborer le profil des personnes cibles et dresser une cartographie des réseaux. Les informations sociales et personnelles de la cible présentent alors un intérêt dans l'optique de mener des attaques d'hameçonnage. Le second objectif serait de découvrir les réseaux et contacts de la personne visée qui pourraient être compromis par les autorités iraniennes[27]. La *personne de contact H* relève que les pirates informatiques iraniens détectent des failles dans les réseaux, ce qui leur permet par exemple d'accéder à des comptes de messagerie[28]. Les pirates informatiques travaillant pour le gouvernement lancent souvent des cyberattaques contre des activistes de la diaspora[29].

Identification facile d'un grand nombre d'utilisatrices et utilisateurs « normaux » et imprudents. De nombreuses personnes exilées d'Iran qui n'avaient aucune activité politique auparavant ont rejoint le mouvement de protestation. Beaucoup de personnes ne dissimulant

21 Un malware ou maliciel est un programme ou logiciel malveillant conçu pour s'installer sur un appareil de la personne concernée à son insu lorsqu'elle clique sur un lien ou une pièce jointe.

22 Les personnes victimes d'hameçonnage ou filoutage sont attirées et trompées par le phishing et amenées dans ce but à se connecter à des sites afin de divulguer leurs données. De faux comptes ou applications sont souvent utilisées à cet effet. Landinfo, Norwegian Country of Origin Information Centre, Iran; Reaksjoner mot iranere i eksil, 28 novembre 2022, p. 16: https://www.ecoi.net/en/file/local/2083379/Temanotat-Iran-Reaksjoner-mot-iranere-i-eksil-28112022.pdf

23 Ibid.

24 BfV, Cyber-Brief Nr. 01/2023, 10 août 2023, p. 1: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2023-01-bfv-cyber-brief-deutsch.pdf?__blob=publicationFile&v=5.

25 Tagesschau, Wie das iranische Regime seine Kritiker hackt, 19 août 2023: https://www.tagesschau.de/ausland/asien/iran-cyberfalle-verfassungsschutz-100.html.

26 Entretien téléphonique du 23 octobre 2023 avec la personne de contact G.

27 CGRA-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10 mai 2023, p. 21.

28 Entretien téléphonique du 27 octobre 2023 avec la personne de contact H.

29 Freedom House, Freedom on the Net 2023 - Iran, 4 octobre 2023.

pas suffisamment leur identité, il est plus facile pour les autorités iraniennes de les surveiller[30]. Dans ce contexte, le président du *Bundesamt für Verfassungsschutz Thomas Haldenwang* a mis en garde contre les activités sur les réseaux sociaux susceptibles de révéler l'identité de personnes critiquant le régime. Le service de renseignement iranien a en effet intérêt à identifier les participant·e·s aux grandes manifestations de solidarité à Berlin. Selon *Haldenwang*, la tâche des services iraniens a encore été facilitée par le fait que les personnes impliquées se soient photographiées et filmées mutuellement pendant la manifestation et qu'elles aient diffusé les images sur les réseaux sociaux. Force est de constater que depuis maintenant plusieurs années, les autorités iraniennes trouvent un intérêt à rechercher des informations sur ces individus[31]. La *personne de contact H* a également signalé que les autorités iraniennes peuvent parfois facilement identifier certains membres de la diaspora actifs sur les réseaux sociaux. De nombreuses personnes seraient très négligentes quant à la divulgation de leurs données personnelles. Lorsque les personnes publient des photos d'elles sur les réseaux sociaux, leur identification s'en trouve ainsi grandement facilitée[32].

Contenu en persan au centre de l'attention. Mais des contenus dans d'autres langues peuvent aussi être surveillés. Selon les indications des *personnes de contact G et E*,[33] l'accent serait mis sur la surveillance des contributions en persan[34]. La *personne de contact C*[35] estime que les contributions dans différentes langues sont aussi surveillées[36].

Comportement des utilisatrices et utilisateurs déterminant pour décider quels réseaux sociaux sont surveillés. Selon les indications concordantes des *personnes de contact H et I*, le comportement des utilisatrices et utilisateurs en Iran est un facteur décisif pour le choix des autorités de surveiller de plus près un réseau social particulier. Instagram, Telegram et Twitter (devenu « X »[37]) seraient actuellement plus populaires que Facebook. L'accent est donc davantage mis sur ces réseaux. Cependant, aucun réseau social ne peut être généralement exclu lorsqu'il s'agit de surveillance[38]. L'*expert en cybersécurité X* a également déclaré que Twitter, Instagram et Telegram sont des réseaux sociaux majeurs pour atteindre le public iranien. Twitter et Instagram seraient les réseaux sociaux les plus importants pour les Iranien·ne·s[39]. Selon l'*expert en cybersécurité X* et la *personne de contact H*, Twitter est une plateforme très politique, tandis qu'Instagram est plutôt utilisé pour le divertissement[40]. Selon la *personne de contact H*, Twitter fait l'objet d'une surveillance accrue et de nombreuses personnes sont arrêtées pour des propos tenus sur cette plateforme. Telegram compte un nombre très élevé d'utilisatrices et utilisateurs d'origine iranienne – près de la moitié de la population du pays – et s'avère de ce fait être également très intéressant pour les autorités

30 Landinfo, Iran: Overvåking av regimekritikere i utlandet som følge av «Kvinne, liv, frihet-protestene», 5 juillet 2023, p. 4: https://www.ecoi.net/en/file/local/2094929/Respons-Iran-Overvaking-av-regimekritikere-i-utlandet-som-folge-av-Kvinne-liv-frihet-protestene-05072023-1.pdf

31 Die Zeit, Verfassungsschutz warnt Menschen iranischer Herkunft vor Ausspähung, 1er janvier 2023: https://www.zeit.de/politik/deutschland/2023-01/verfassungschutz-ausforschung-iran-regimekritiker-deutschland.

32 Entretien téléphonique du 27 octobre 2023 avec la personne de contact H.

33 La personne de contact E, d'origine irano-allemande, dispose de connaissances spécialisées sur l'Iran.

34 Entretiens téléphoniques du 23 et 24 octobre 2023 avec les personnes de contacts G et E.

35 La personne de contact C est un·e militant·e politique et membre de la diaspora iranienne.

36 Entretien téléphonique du 26 octobre 2023 avec la personne de contact C.

37 Twitter a été renommé « X » en été 2023.

38 Entretiens téléphoniques du 27 octobre et du 15 septembre 2023 avec les personnes de contact H et I.

39 CGRA-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10 mai 2023, p. 21-22.

40 Ibid.; entretien téléphonique du 27 octobre 2023 avec la personne de contact H.

iraniennes. Suite à plusieurs fuites d'informations de comptes dans le passé, les autorités iraniennes disposent déjà de nombreuses données provenant d'utilisatrices et utilisateurs de Telegram et continuent activement d'obtenir des données d'autres Iranien·ne·s au moyen de fausses pages de connexion ou d'imitations d'applications[41]. Selon l'*expert en cybersécurité X*, les blogs et Facebook ne sont plus populaires en Iran et ont par conséquent perdu de leur intérêt pour les autorités iraniennes[42].

3 Groupes à risque

Les priorités des autorités iraniennes concernant les groupes surveillés sont susceptibles de changer. Selon l'*expert en cybersécurité X* spécialiste de l'Iran, les autorités iraniennes surveillent les activistes en exil. Elles n'auraient toutefois pas la capacité d'en surveiller la totalité. Le régime fixe ainsi des priorités en fonction de ses intérêts, et ces priorités peuvent varier[43].

Toutes formes d'organisation politique et réseaux de la diaspora en point de mire des autorités iraniennes. La *personne de contact I*[44] a informé l'OSAR que l'attention des autorités iraniennes était dirigée vers toutes les formes d'organisation politique au sein de la diaspora. Les réseaux de la diaspora sont certainement surveillés. Selon la *personne de contact I*, dès qu'il s'agit d'organisations et de réseaux de la diaspora formés sur Internet, il convient de partir du principe que les autorités iraniennes surveillent toujours leurs activités sur les réseaux sociaux[45].

Landinfo signale que la surveillance et les cyberattaques peuvent toucher un large groupe d'Iranien·ne·s en exil[46]. Différents profils mentionnés dans les sources sont énumérés dans la liste ci-dessous :

- **les victimes de cyberattaques sont des opposant·e·s au régime iranien.** Selon *Jadran Mesic, le chef du département de cyberdéfense du Bundesamt für Verfassungsschutz*, les personnes s'opposant « manifestement » au régime iranien qui communiquent ouvertement leurs opinions critiques et sont de ce fait connues des autorités iraniennes figurent parmi les victimes de cyberattaques en Allemagne. Il existerait en outre un rapport avec le fait d'entretenir des liens étroits avec certaines organisations, par exemple de défense des droits humains, en Iran[47]. *Shiva Mahbobi, porte-parole de la Campaign to Free Political Prisoners in Iran*, suppose également que les activistes critiques à l'égard du gouvernement sont surveillé·e·s[48].

41 Entretien téléphonique du 27 octobre 2023 avec la personne de contact H.
42 CGRA-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10 mai 2023, p. 21-22.
43 Ibid., p. 21.
44 La personne de contact I dispose de connaissances spécialisées en matière de répression transnationale et de surveillance numérique par l'État iranien.
45 Entretien téléphonique du 15 septembre 2023 avec la personne de contact I.
46 Landinfo, Iran; Reaksjoner mot iranere i eksil, 28 novembre 2022, p. 23.
47 Tagesschau, Wie das iranische Regime seine Kritiker hackt, 19 août 2023: https://www.tagesschau.de/ausland/asien/iran-cyberfalle-verfassungsschutz-100.html.
48 CGRA-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10 mai 2023, p. 23.

- **les journalistes.** Diverses sources rapportent que les journalistes, y compris celles et ceux qui travaillent pour des médias réformateurs ou des médias étrangers, sont susceptibles de devenir la cible de cyberattaques ou de surveillance[49].
- **les derviches Gonabadi, les dissident·e·s azerbaïdjanais·e·s, les activistes des droits des femmes et les étudiant·e·s.** Parmi les victimes d'attaques de logiciels malveillants visant à cibler des groupes spécifiques à l'intérieur et à l'extérieur du pays et à collecter des informations privées figurent aussi les derviches Gonabadi, les personnes dissidentes azerbaïdjanaises, les activistes des droits des femmes ainsi que les militant·e·s étudiant·e·s[50].
- **les organisations dissidentes, les juristes et les activistes des droits humains.** En 2022, plusieurs prestataires de services de sécurité informatique ont mentionné l'implication du groupe *Charming Kitten* dans les recherches visant des opposant·e·s au régime et des Iranien·ne·s en exil. Les cyberattaques visaient principalement des organisations dissidentes et des personnes déterminées telles que des juristes ou des activistes des droits humains, en Iran et à l'étranger[51]. Selon le *contact G*, les personnes collectant des informations relatives à des violations des droits humains en Iran peuvent aussi se retrouver visées par une surveillance numérique[52].
- **les activistes des minorités ethniques et les activistes écologistes.** L'*expert en cybersécurité X* a informé CEDOCA que les activistes issu·e·s des minorités ethniques et les activistes de l'environnement se retrouvent, entre autres, victimes d'attaques de pirates informatiques[53].
- **les fonctionnaires du gouvernement iranien et les politicien·ne·s favorables aux « réformes »**, tels que les membres du gouvernement des anciens présidents Hassan Rohani et Mahmoud Ahmadinejad[54].
- **les minorités religieuses**, y compris les membres de la foi Baha'i, mais aussi les personnes et institutions chrétiennes, juives, zoroastriennes ou musulmanes sunnites[55].
- **les personnalités culturelles** telles que les artistes, les musicien·ne·s, les caricaturistes et les satiristes[56].
- **les groupes d'opposition, les organisations terroristes, les groupes ethniques séparatistes et les organisations de la société civile basées à l'étranger** [57].

Personnes appartenant à l'environnement social des personnes cibles. Les attaques tentant de soutirer des données et dérober les identifiants de connexion aux comptes de messagerie et de réseaux sociaux des victimes visent souvent des groupes ou réseaux plus larges autour de personnes spécifiques. Cela augmente les chances de réussite et les probabilités d'accéder à des données qui peuvent mettre en danger l'ensemble du réseau[58]. Le

49 Ibid., p. 21; entretiens téléphoniques du 23 octobre et du 15 septembre 2023 avec les personne de contact G et I; BfV, Cyber-Brief Nr. 01/2023, 10 août 2023, p. 1; Landinfo, Iran; Reaksjoner mot iranere i eksil, 28 novembre 2022, p. 23.
50 Freedom House, Freedom on the Net 2023 - Iran, 4 octobre 2023.
51 BfV, Cyber-Brief Nr. 01/2023, 10 août 2023, p. 1.
52 Entretien téléphonique du 23 octobre 2023 avec la personne de contact G.
53 CGRA-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10 mai 2023, p. 21.
54 Landinfo, Iran; Reaksjoner mot iranere i eksil, 28 novembre 2022, p. 23.
55 Ibid.
56 Ibid.
57 Ibid.
58 Ibid.

service de renseignement iranien peut également s'intéresser à toutes les formes d'informations susceptibles d'être utilisées pour faire pression sur des individus, comme les informations sur la consommation d'alcool ou les relations sexuelles[59]. Cela signifie que les personnes appartenant au cercle social des personnes visées peuvent aussi être surveillées par les services secrets[60].

Cyberattaques plutôt dirigées contre des dissident·e·s d'un niveau élevé, alors que la surveillance inclut aussi des personnes au moindre profil. Selon *l'expert iranien en cybersécurité Y*, la manière dont les autorités iraniennes surveillent les Iranien·ne·s à l'étranger dépend de la cible. Les autorités iraniennes ont ciblé quelques dissident·e·s de premier plan au sein de la diaspora par le biais de logiciels malveillants. Le régime pourrait considérer les activistes politiques de haut niveau comme une menace et lancer à leur encontre des attaques sophistiquées en matière de cybersécurité. Selon l'*expert Y*, il serait peu probable que les autorités iraniennes considèrent les personnes ayant simplement participé à des manifestations à l'étranger comme des cibles de haut rang pour mener des cyberattaques élaborées[61]. Le *contact H* a également souligné que les autorités iraniennes visent les personnes de faible profil dans des opérations telles que l'hameçonnage et le piratage de courriels uniquement si elles font partie d'un réseau plus vaste[62]. Toutefois, selon l'*expert Y*, il est tout à fait possible que les profils sur les réseaux sociaux de personnes qui ne sont pas des dissident·e·s de haut niveau soient surveillés. Les autorités iraniennes peuvent par exemple lire ce qu'une personne *tweete* ou voir qui fait partie de son réseau. L'*expert Y* a précisé que les autorités iraniennes utiliseraient à cette fin les informations accessibles au public et ne surveilleraient pas les comptes privés[63].

3.1 Direction d'un groupe

Les autorités se concentrent davantage sur les leaders et les activistes politiques. La *personne de contact G* a indiqué à l'OSAR que l'intensité de la surveillance des activités sur les réseaux sociaux dépendait du profil de la personne visée. Si le gouvernement estime que la personne concernée est une cible, elle fera éventuellement l'objet d'une surveillance. Si elle n'est qu'une simple participante à une manifestation à l'étranger et n'est pas perçue comme influente par les autorités iraniennes, le gouvernement ne surveillera probablement pas ses activités sur les réseaux sociaux. Selon le *contact G*, les autorités iraniennes s'en prennent plutôt aux personnes qui mènent des manifestations ou qui sont des activistes de l'opposition[64]. L'*expert iranien en cybersécurité Y* a déclaré que les autorités iraniennes ciblent les principaux leaders et les organisatrices et organisateurs de la diaspora iranienne, c'est-à-dire les personnes qui dirigent un groupe ou un parti, et les personnes dont les activités sont suivies et reconnues par un groupe de personnes[65].

---

59 Immigration and Refugee Board of Canada (IRB), Iran: Treatment by the authorities of anti-government activists, including those returning from abroad; overseas monitoring capabilities of the government (2019–February 2021, 22 février 2021: https://www.ecoi.net/de/dokument/2047908.html.

60 Landinfo, Iran; Reaksjoner mot iranere i eksil, 28 novembre 2022, p. 23.

61 CGRA-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10 mai 2023, p. 22.

62 Entretien téléphonique du 27 octobre 2023 avec la personne de contact H.

63 CGRA-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10 mai 2023, p. 22.

64 Entretien téléphonique du 23 octobre 2023 avec la personne de contact G.

65 CGRA-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10 mai 2023, p. 22.

Des exceptions sont possibles et des personnes inconnues peuvent être ciblées par hasard ou par erreur. La *personne de contact G* a cependant affirmé qu'il existe des exceptions en fonction des activités de la personne sur les réseaux sociaux ou ailleurs. Cette source a souligné que les services de sécurité iraniens pouvaient par exemple se tromper dans leur évaluation. Ils pourraient ainsi prendre à tort une personne pour un·e leader et la cibler. La *personne de contact G* a cité en exemple le cas d'une étudiante iranienne aux États-Unis. Elle n'était en aucun cas une figure importante de l'opposition, mais elle avait été invitée à une émission de télévision d'*Iran International* en relation avec les récentes manifestations de la diaspora. Elle s'est alors retrouvée dans le collimateur des services de sécurité iraniens[66]. La *personne de contact H* a déclaré que les services de renseignement iraniens s'en prennent occasionnellement à des personnes inconnues : « personne ne sait qui elles sont, mais, pour une raison quelconque, les autorités iraniennes ont de l'intérêt à les suivre »[67]. Les autorités peuvent en outre découvrir une personne par hasard, parce qu'elle a participé à une discussion qui était déjà dans leur ligne de mire[68].

Les personnes qui dirigent des groupes de cinq personnes peuvent par exemple déjà se retrouver dans le collimateur des autorités. Il n'est pas nécessaire qu'il s'agisse de « leaders importants ». La *personne de contact G* fait référence aux recherches du *Miaan Group*, qui a documenté des cas de surveillance numérique. Les personnes n'ont pas nécessairement besoin d'être à la tête d'un groupe important pour être ciblées par les services de renseignement iraniens. Cinq personnes ont par exemple suffi à attirer l'attention des autorités. La *personne de contact G* a souligné qu'il ne devait pas forcément s'agir de « leaders importants ». Toute personne présente sur les réseaux sociaux peut ainsi se retrouver, ne serait-ce que par hasard, dans le collimateur des autorités. Mais en principe, on peut supposer qu'une personne ayant beaucoup de *followers* sur les réseaux sociaux sera plus facilement ciblée[69].

Les personnes jouissant d'une « grande notoriété », les personnes dirigeant un groupe et les personnes influentes sont systématiquement surveillées. La *personne de contact G* a souligné qu'une personne très populaire jouissant d'une « forte notoriété » sur les réseaux sociaux sera surveillée. Le degré de véracité des contenus diffusés ne joue aucun rôle. Certaines personnes « publient des immondices » et sont suivies, parce que les gens s'intéressent à ces sujets. Elles deviennent ainsi automatiquement des personnes d'influence. Peu importe ses dires ou ses activités, s'éloigner des intérêts de l'Iran suffit à devenir une cible. Lorsqu'une personne bénéficie d'une « grande notoriété », dirige un groupe ou exerce une certaine influence, elle sera surveillée en permanence et de manière systématique[70].

3.2 Portée

Du point de vue iranien, l'influence ne se définit pas seulement par le nombre de *followers*, mais aussi par la capacité d'une personne à lancer une tendance ou un débat. La *personne de contact H* a souligné que les autorités iraniennes traquent généralement les

66 Entretien téléphonique du 23 octobre 2023 avec la personne de contact G.
67 Entretien téléphonique du 27 octobre 2023 avec la personne de contact H.
68 Entretien téléphonique du 23 octobre 2023 avec la personne de contact G.
69 Ibid.
70 Ibid.

personnes qu'elles considèrent comme influentes. Selon elle, il conviendrait toutefois de noter qu'en Iran, la définition de la notion d'influenceur est totalement différente de celle des États-Unis ou de l'Europe. En Iran, être influenceur ne signifie pas avoir 10 000 abonné·e·s. Le point focal serait plutôt que la personne puisse déclencher une tendance ou un débat sur un thème donné. Si une personne entre dans cette catégorie, les autorités iraniennes tenteront de la retrouver[71]. L'*expert en cybersécurité X* indique également que l'influence qu'exerce une personne est déterminante pour savoir si elle suscite l'intérêt des autorités iraniennes. Il peut s'agir par exemple d'une personne apparaissant sur des chaînes de télévision comme *Iran International* ou *VOA*. Contrairement à la *personne de contact H*, l'*expert en cybersécurité X* considère que le meilleur critère pour mesurer l'influence serait le nombre de *followers*. Cependant, il n'existe pas de formule simple permettant de mesurer l'influence. Dans un cas, 10 000 abonné·e·s ne représenteraient peut-être pas grand-chose, tandis que 50 000 ou 100 000 seraient plus significatifs. Il faut par ailleurs tenir compte du fait que les abonné·e·s peuvent être acheté·e·s. Dans le cas où une personne n'a que peu de *followers*, le fait qu'une contribution soit *retweetée* par 500 personnes peut être significatif. Si tous les *tweets* d'une personne sont par exemple *retweetés* 100 fois, alors cette personne serait une influenceuse ou un influenceur. Lorsqu'une personne est capable d'exercer de l'influence sur la couverture médiatique, elle devient intéressante pour les autorités iraniennes. Le facteur décisif réside dans la manière dont une personne peut faire avancer un récit. Les autorités iraniennes persécutent des personnes dont « la voix est entendue »[72]. La *personne de contact H* a également souligné que le nombre de vues d'une publication pouvait être un facteur important pour attirer l'attention des autorités. Selon la *personne de contact H*, même si une personne partage et renforce un discours dont elle n'est pas à l'origine, les autorités la remarqueront et la cibleront[73].

Une plus grande portée entraîne probablement davantage de répression. Selon la *personne de contact I*, les personnes qui ont une plus grande portée publique font l'objet de mesures plus strictes, car elles sont perçues comme des ennemis visibles. Elles sont menacées en ligne et leurs familles en Iran sont également menacées[74]. La *personne de contact G* estime aussi que les autorités agissent de manière plus répressive lorsqu'une personne concernée a plus de *followers*[75].

Outre la portée et la direction d'un groupe, la connexion ou la communication avec un groupe peut être un facteur. En plus des éléments principaux pouvant conduire à une surveillance que sont la portée et le fait de diriger un groupe, les autres critères dépendraient, selon la *personne de contact G*, de chaque cas particulier. Il s'agit notamment de savoir si la personne est en contact ou communique avec un autre groupe. Les autorités effectueraient de surcroît des recherches supplémentaires afin de déterminer si elles souhaitent cibler une personne[76].

3.3 Propos

71 Entretien téléphonique du 27 octobre 2023 avec la personne de contact H.
72 CGRA-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10 mai 2023, p. 21.
73 Entretien téléphonique du 27 octobre 2023 avec la personne de contact H.
74 Entretien téléphonique du 15 septembre 2023 avec la personne de contact I.
75 Entretien téléphonique du 23 octobre 2023 avec la personne de contact G.
76 Ibid.

Les « lignes rouges » du contenu peuvent changer à tout moment. Dans une étude, *Marcus Michaelsen* a interrogé un grand nombre d'activistes de la diaspora sur la surveillance numérique exercée par les États autoritaires. Les entretiens avec les personnes interrogées ont permis de mettre en évidence certaines des limites qui, si elles sont dépassées, pourraient provoquer une réaction des autorités. Parmi les sujets abordés figuraient les personnalités du régime, les organes de sécurité, les prisonniers politiques, la torture, la corruption, les problèmes économiques et les minorités ethniques et religieuses. Plusieurs personnes interrogées ont relevé que « tout pourrait être une ligne rouge », et qu'il vaudrait mieux « ne pas s'exprimer du tout ». *Michaelsen* remarque en particulier que ces « lignes rouges » peuvent changer à tout moment en fonction de la situation et du contexte. Cet exercice arbitraire du pouvoir est une caractéristique inhérente aux régimes autoritaires et favorise la peur et l'autocensure parmi les citoyen·ne·s, même au-delà des frontières[77].

Le cumul des critiques n'est probablement pas un facteur essentiel. Selon *l'expert en cybersécurité X*, la quantité de critiques émises par une personne à l'encontre du régime ne serait pas un facteur significatif augmentant le risque de surveillance. C'est plutôt « l'influence » de la personne concernée qui serait déterminante[78].

Probablement sans importance que les propos partagés soient personnels ou qu'il s'agisse de contributions de tiers. Selon les *personnes de contact H et I*, il ne serait pas pertinent de faire une distinction entre le partage de ses propres déclarations et le partage de contenus de tiers[79]. En cas de doute, les autorités iraniennes peuvent tout utiliser contre la personne. Il s'avère dès lors difficile d'évaluer ce qui attire l'attention des autorités. Lorsqu'une personne a partagé quelque chose, cela peut être utilisé à son détriment pour la pousser à collaborer avec les services de renseignement[80]. Selon la *personne de contact G*, il n'est pas possible de dire avec une certitude absolue si les mesures de répression iraniennes diffèrent lorsqu'une personne partage ses propres contributions ou des contenus de tiers. D'après l'expérience de l'organisation de la *personne de contact G* et les informations dont elle dispose, le simple fait de partager une déclaration n'entraîne généralement pas de se retrouver dans le collimateur des services de sécurité iraniens. La *personne de contact G* a toutefois admis qu'il n'était pas possible de le déterminer avec certitude[81]. Selon la *personne de contact H*, il est probablement plus important de savoir si la personne est une influenceuse ou un influenceur au sens de la définition iranienne[82]. La *personne de contact G* a cependant souligné qu'une personne qui n'est pas considérée comme influenceuse ou influenceur et qui ne fait que partager un contenu de tiers peut tout de même se retrouver dans le collimateur des services de renseignement iraniens[83].

Les autorités iraniennes agissent parfois de manière imprévisible et même une personne inconnue peut être arrêtée à son retour. La *personne de contact G* a indiqué que cela ne dépend pas nécessairement des propos partagés par la personne dans un média

77 Michaelsen, Marcus, Silencing Across Borders, Transnational Repression and Digital Threats against Exiled Activists from Egypt, Syria, and Iran, 2020, p. 13.
78 CGRA-CEDOCA, Iran; Surveillance van de diaspora door de Iraanse autoriteiten, 10 mai 2023, p. 21.
79 Entretiens téléphoniques du 27 octobre et du 15 septembre 2023 avec les personne de contact H et I.
80 Entretien téléphonique du 15 septembre 2023 avec la personne de contact I.
81 Entretien téléphonique du 23 octobre 2023 avec la personne de contact G.
82 Entretien téléphonique du 27 octobre 2023 avec la personne de contact H.
83 Entretien téléphonique du 23 octobre 2023 avec la personne de contact G.

social. Il est très compliqué de prédire si et quand une personne sera prise pour cible[84]. La *personne de contact H* a relevé que l'approche des autorités iraniennes n'était pas toujours logique. Ainsi, alors que tout pourrait indiquer un risque élevé, il est possible que rien ne se passe en cas de retour. La *personne de contact H* connaît toutefois aussi quelques exemples inverses. Dans un cas, des personnes se sont retrouvées en danger à cause d'un message aléatoire publié sur les réseaux sociaux. Même si une personne n'est pas un « gros poisson » et n'a *liké* que certains membres éminents de la diaspora ou quelques propos critiques dans les médias sociaux, il se peut que les autorités l'arrêtent à son retour. Les autorités iraniennes pourraient aussi « inventer » un dossier afin de poursuivre une personne en justice[85].

84 Ibid.
85 Entretien téléphonique du 27 octobre 2023 avec le contact H.