PRIVACY INTERNATIONAL

Les Yeux du Pouvoir

Rencontres avec des citoyens marocains sous-surveillance

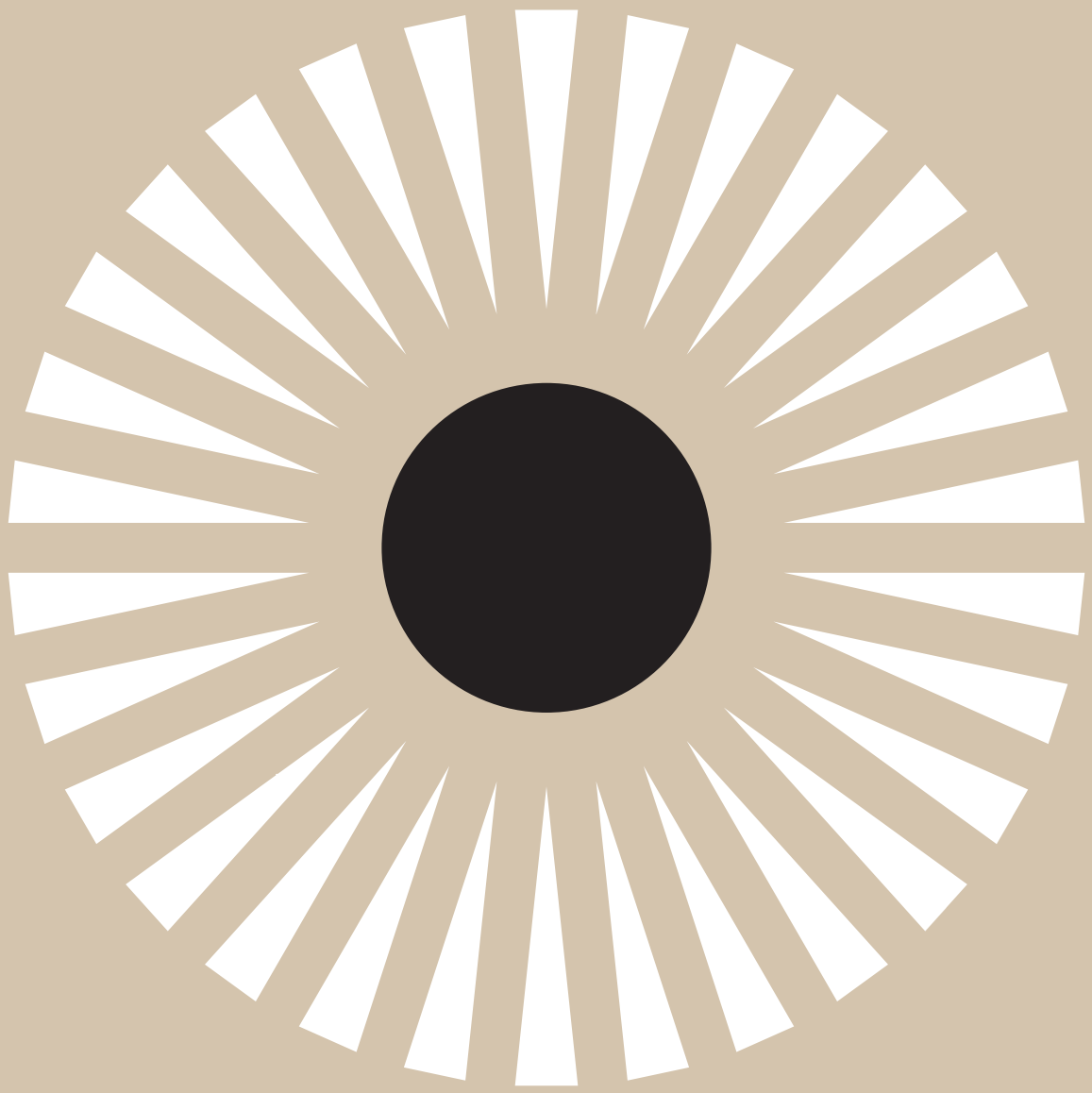

Photo © Anthony Drugeon

Les Yeux du Pouvoir

Rencontres avec des citoyens marocains sous-surveillance

PRIVACY INTERNATIONAL

www.privacyinternational.org

Photo © Anthony Drugeon

Sommaire

Photo © Anthony Drugeon

Avant-Propos

Privacy International est une organisation caritative qui a pour objectif de défendre le droit à la vie privée à travers le monde. Nous enquêtons sur l'univers secret de la surveillance gouvernementale et dévoilons le rôle des entreprises qui permettent cette surveillance. Nous menons des actions en justice afin que la surveillance soit toujours pratiquée dans le cadre de la loi. Nous prônons l'adoption de lois solides à l'échelle régionale, nationale et internationale pour protéger la vie privée. Nous produisons des recherches qui font évoluer les politiques en place. Nous alertons le public sur les technologies et les lois qui mettent en danger la vie privée – afin que nous puissions tous être informés et prendre position.

Nous sommes fiers de l'étendue de notre travail avec nos partenaires du monde entier. Nous travaillons en particulier depuis un an dans 13 pays, afin d'aider des organisations locales à développer leurs compétences en termes d'investigation et de campagnes en faveur de la protection de la vie privée dans leurs pays.

Le Maroc est un pays sur lequel nous avons porté une attention toute particulière. Nos rencontres, avec des militants engagés dans la défense d'Internet et du secret de la correspondance, nous ont poussés à orienter nos efforts vers ce pays. Hisham Almiraat – un militant acharné pour le droit à la vie privée, lui-même victime de la surveillance – a été en première ligne de ce combat, avec sa nouvelle organisation, l'Association des Droits Numériques.

Nous vous présentons dans ce rapport les récits de quatre citoyens marocains, dont Hisham, placés sous surveillance, et l'impact que cela a eu sur leurs vies et celles de leurs familles.

Nous pensons que ces portraits en disent beaucoup sur le contexte actuel de la surveillance au Maroc. Nous espérons qu'ils deviendront le déclencheur d'un débat public indispensable au Maroc sur ces questions. Un débat que nous souhaitons d'ailleurs voir émerger au-delà du Maroc, alors que nous faisons tous face aux dangers de la surveillance non-réglementée.

Privacy International et l'Association des Droits Numériques

Introduction

De par sa nature, la surveillance donne du pouvoir à ceux qui l'exercent. Si elle est secrète, elle devient donc dangereuse parce que nous ne pouvons plus contrôler ce pouvoir. Les dommages de la surveillance secrète ne sont pas toujours connus par ceux qui en sont les victimes et le droit à la vie privée est d'ailleurs l'un des rares droits dont la violation ne laisse parfois aucune trace. Il arrive qu'il soit impossible d'identifier le responsable.

Voir son espace personnel envahi et observé est quelque chose de tout à fait déstabilisant. C'est un peu comme si une personne se cachait dans le noir et, où que vous alliez, cette personne enregistre tout ce que vous faites. Avec les technologies d'aujourd'hui, il y a de fortes chances pour que vous ne remarquiez jamais cette personne, que vous ne sachiez jamais son nom, que vous ne voyiez jamais son visage ou connaissiez ses intentions.

Il est donc rare de rencontrer des victimes de la surveillance, et encore plus de savoir comment elles ont été espionnées, dans quel but et par qui. Depuis plus d'un an, Privacy International a rencontré des militants et des journalistes marocains qui ont été espionnés par le gouvernement et des organisations associées au pouvoir. Grâce à l'Association des droits numériques – notre partenaire local – nous pouvons désormais retracer plusieurs cas dérangeants de surveillance particulièrement intrusive au Maroc.

Certaines victimes ont été visées par un logiciel espion extrêmement onéreux de la société italienne de surveillance Hacking Team. Selon un rapport publié en 2014 par Citizen Lab – le groupe de recherches interdisciplinaires de l'université de Toronto – Hacking Team aurait vendu son logiciel espion Remote Control System à 21 pays. Parmi ces pays figuraient l'Azerbaïdjan, l'Égypte, l'Éthiopie, le Kazakhstan, l'Arabie Saoudite et le Soudan, tous connus pour leur peu de considération à l'égard des droits de l'homme.

Dans d'autres cas, la surveillance au Maroc se fait par un « passage en force numérique. » Des journalistes et des militants ont ainsi vu leurs adresses email et comptes Facebook piratés par des groupes de hackers nationalistes. Ces activités illégales sont par ailleurs restées impunies.

Mais la surveillance s'effectue aussi par des tactiques policières plus traditionnelles – mais non moins intimidantes et douteuses d'un point de vue légal. Des récits de voisins et de proches visités par les forces de l'ordre pour obtenir des informations – ou simplement pour intimider les militants – nous ont été racontés à de multiples reprises. Des cas d'écoutes téléphoniques nous ont aussi été décrits.

Le but de la surveillance : empêcher un Printemps marocain

Les histoires qui suivent prennent tout leur sens lorsqu'elles sont lues à la lumière de ce que l'on sait sur le Maroc. L'Etat a en effet investi massivement dans l'espionnage de ses citoyens afin de surveiller leurs activités et de réprimer toute forme de dissidence.

Le Maroc est officiellement une monarchie parlementaire constitutionnelle. Les Marocains élisent leurs députés tous les cinq ans. Mais l'exécutif – représenté par le roi – a un pouvoir très étendu. La monarchie et les conflits dans la zone du Sahara occidental – une zone rebelle revendiquée par le gouvernement marocain – font partie des sujets les plus sensibles au Maroc. La liberté d'expression reste d'ailleurs un des problèmes majeurs dans le pays, un constat qui a été déploré maintes fois par diverses organisations non-gouvernementales.

Le Maroc arrive 116e (sur 167 pays) dans le classement mondial de la démocratie réalisé par la branche Intelligence Unit de la revue anglaise *The Economist*. Ce classement se base sur des critères comprenant le processus électoral et le pluralisme politique, le fonctionnement des institutions et les libertés civiles.

Privacy International a par ailleurs constaté la multiplication des interdictions des activités organisées par les ONG en 2014. Nous avons nous-mêmes été confrontés à ce nouveau problème. Les deux ateliers organisés par notre partenaire local, et que nous parrainions, ont ainsi dû être déplacés à la dernière minute suite à des pressions de la police sur les gérants des salles que nous avions louées. Ces salles se trouvaient au demeurant dans des hôtels appartenant à des chaînes internationales.

De précédentes révélations avaient déjà mis en lumière l'achat en 2011 par le gouvernement marocain des infrastructures de surveillance Eagle pour une valeur de 2 millions d'euros. Eagle permet au gouvernement de censurer Internet et de surveiller le trafic Internet, en utilisant une technologie nommée Deep Packet Inspection. Eagle a été vendu au Maroc par Amesys Bull, une entreprise française tristement célèbre pour avoir vendu une technologie du même type à la Lybie, alors sous le régime du colonel Kadhafi.

Plus récemment – suite à des demandes de Privacy International et de journalistes suisses – le gouvernement helvétique a publié la liste des pays qui ont acheté des technologies de surveillance à des sociétés suisses. Le Maroc figurait parmi les acheteurs et il semblerait que le gouvernement ait testé des technologies d'interception de télécommunications mobiles ou du matériel de brouillage en 2013 et 2014.

La surveillance au Maroc semble avoir joué un rôle à l'importance croissante depuis le Printemps arabe. Au Maroc, l'année 2011 a été marquée par le mouvement du 20 Février, une série de manifestations réclamant plus de démocratie et de transparence de la part du gouvernement.

La police s'est montrée très encline à identifier tout militant impliqué de près ou de loin avec le mouvement. Certains militants que nous avons interviewés nous ont raconté comment la police avait « rendu visite » à leurs proches et leurs voisins pour les questionner sur leurs liens avec le mouvement du 20 Février.

Maria Moukrim est une célèbre journaliste et la rédactrice en chef de la publication Febrayer (« Février »). Son site est devenu à son lancement en 2012 la cible d'un groupe de hackers nationalistes. Mme Moukrim nous a expliqué que son site avait spécifiquement été visé car les hackers pensaient qu'il était directement affilié au mouvement du 20 Février.

«Ils pensaient que ça allait être le site officiel du mouvement du 20 Février. Ils ont piraté mon compte Gmail pour obtenir le mot de passe du serveur et ils ont acheté tous les noms de domaine qui contenaient le mot « Febrayer. » Ensuite ils ont piraté mon compte Facebook et ont posté des contenus obscènes. Ils ont ensuite redirigé toutes les adresses URL « Febrayer » vers mon compte Facebook piraté. C'était extrêmement traumatisant pour le lancement de ma publication.»

200 000 € : le prix de la vie privée d'un journaliste

Ce rapport a avant tout vocation à retracer les expériences de quatre journalistes et militants qui ont chacun été visé par la surveillance de l'Etat. Trois d'entre eux – Hisham Almiraat, Samia Errazzouki et Yassir Kazar – faisaient partie de Mamfakinch, un collectif de citoyens reporters critiques à l'égard du régime, créé parallèlement au mouvement du 20 Février.

Mamfakinch a été visé par un logiciel espion développé et commercialisé par Hacking Team. Unemail avait été envoyé via la page « Contact » du site et transmis à toute la rédaction. Le message laissait entendre que la pièce jointe contenait des révélations majeures. Elle renfermait en réalité le logiciel espion, qui permet à l'attaqueur d'obtenir à distance un accès intégral à l'ordinateur visé. Un logiciel espion de ce type permet ainsi :

- D'avoir accès à tous les fichiers de l'ordinateur visé ;
- D'espionner en temps réel l'usage qui est fait de l'ordinateur et de voir ce qui apparaît sur l'écran ;
- D'enregistrer toutes les touches sur lesquelles l'utilisateur tape, révélant ainsi les mots de passe saisis ;
- De faire des captures d'écrans ;
- D'enclencher la caméra pour prendre des photos et faire des vidéos sans que l'utilisateur le remarque.

Le logiciel espion est estimé à 200 000 €. Hacking Team déclare vendre uniquement ses logiciels à des gouvernements et à des services de police.

Depuis février 2014, Mamfakinch ne publie plus. L'équipe est divisée sur ce qui a conduit à cet arrêt. Pour certains, il s'agissait d'une pause nécessaire alors que le mouvement du 20 Février qu'ils avaient vocation à couvrir avait pris fin. Mais pour d'autres, dont le cofondateur Hisham Almiraat, l'équipe s'est peu à peu dispersée par peur des conséquences. L'utilisation du logiciel espion de Hacking Team avait d'un coup augmenté les risques : si le gouvernement était prêt à investir de tels montants pour découvrir qui était derrière le collectif, ceux qui avaient une carrière à protéger

sentait qu'il était peut-être temps pour eux de se retirer.

Milices hackers : citoyens zélés ou agents de renseignement ?

Le quatrième portrait est celui d'une personnalité bien connue au Maroc, Ali Anouzla. Ali Anouzla est un journaliste d'investigation et le rédacteur en chef du média indépendant en ligne Lakome, bloqué par le gouvernement marocain depuis octobre 2013 et accessible seulement via des sites miroirs. Les articles d'Ali Anouzla ont fréquemment mécontenté le régime : il a en effet toujours fait partie des rares journalistes qui ont osé écrire sur la monarchie et a souvent enquêté sur les scandales de corruption. Mais c'est seulement en 2013 que son histoire traverse les frontières : après avoir été emprisonné suite à des poursuites pour « apologie du terrorisme. »

Ali Anouzla avait en fait posté un lien vers un article du quotidien espagnol El Pais qui contenait une vidéo d'Al Qaida, le sujet de son article. Ali Anouzla, ainsi que de nombreux observateurs, estiment que cette arrestation était liée à son article révélant que le roi avait accordé le pardon royal à un pédophile espagnol emprisonné dans une prison marocaine. L'information avait causé un véritable tollé au Maroc et avait conduit à des émeutes dans la capitale.

Le récit d'Ali Anouzla révèle l'existence d'un réseau de milices hackers – les mêmes qui s'en étaient pris à la publication de Maria Moukrim – prétendant défendre les valeurs du Maroc en piratant les sites et les comptes personnels des opposants au régime. Ces groupes ont diverses appellations : Les Jeunesses monarchistes, les Forces de répression marocaine, Moroccan Ghosts ou encore les Brigades royales de dissuasion. Certains ont aussi visé des sites algériens et israéliens, des pays considérés comme des ennemis du Maroc.

Si les financements potentiels de ces groupes – et leurs liens avec le gouvernement – demeurent obscurs, il est important de garder à l'esprit que leurs activités sont encouragées par des médias suspectés d'être liés aux services secrets.

De l'espoir pour le Maroc

Nous espérons que cette série de portraits aidera à enclencher un débat nécessaire au Maroc sur la question de la surveillance des journalistes et des militants. Ces récits prouvent plus que jamais que le droit à la vie privée est une composante essentielle de la démocratie.

Ce rapport est une rare opportunité de partir à la rencontre de ceux dont les vies ont été entravées par la surveillance. Certains sont méfiants, d'autres indignés. Mais tous s'accordent pour dénoncer ce qu'il leur est arrivé et réclament justice. Nous espérons que leurs récits et nos efforts – mêmes minimes – contribueront à leur combat pour une société libre, ouverte et démocratique.

Méthodologie

Cette introduction a été rédigée par le personnel Privacy International en Février 2015. Elle est basée sur des interviews d'Hisham Almiraat, Ali Anouzla, Ahmed Benseddik, Samia Errazzouki, Yassir Kazar et Maria Moukrim. Les interviews sont à lire dans les chapitres suivants de ce rapport.

Ci-dessous vous trouverez les liens vers les articles et les recherches mentionnés dans l'article, ainsi que des lectures que nous vous recommandons.

Pour en savoir plus sur Hacking Team

- https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/ (EN ANGLAIS)
- http://owni.fr/2012/09/14/lespion-etait-dans-le-doc/

Le classement mondial de la démocratie d'Intelligence Unit (The Economist)

- http://www.eiu.com/public/topical_report.aspx?campaignid=Democracy0115 (EN ANGLAIS)

Pour en savoir plus sur les interdictions gouvernementales des activités d'ONG

- http://www.amdh.org.ma/fr/communiques/liste-des-interdictions-des-activites-de-l-amdh-depuis-juillet-2014
- http://telquel.ma/2014/12/18/embargo-lassociation-adala-empechee-fois-dorganiser-reunion-les-autorites_1426709
- http://www.hespress.com/societe/239347.html (EN ARABE)

Pour en savoir plus sur l'achat d'Eagle par le gouvernement marocain

- http://reflets.info/amesys-un-finger-de-pop-corn-pour-le-croco/
- http://reflets.info/maroc-le-meilleur-ami-de-la-france-se-met-au-dpi-grace-a-amesys-la-filiale-de-bull/

Pour en savoir plus sur les documents du gouvernement suisse concernant les exportations de technologies à double usage

- https://www.privacyinternational.org/?q=node/98 (EN ANGLAIS)

Pour en savoir plus sur les manifestations qui ont suivi le pardon royal d'un pédophile espagnol

- http://www.theguardian.com/world/2013/aug/04/dozens-injured-morocco-protest-spanish-paedophile (EN ANGLAIS)

Pour en savoir plus sur les groupes de hackers marocains

- http://www.slateafrique.com/97729/qui-se-cache-derriere-moroccan-ghosts-hacker-cyber-activiste

Les groupes de hackers marocains sur les réseaux sociaux

- https://twitter.com/moroccankingdom (Compte Twitter des Forces de Répression marocaine)
- https://twitter.com/moroccanghosts (Compte Twitter des Moroccan Ghosts)
- https://www.facebook.com/pages/-الدرع-لقوات-اللواء-حملة/المغربية398791140150215?sk=timeline&ref=page_internal (Page Facebook des Brigades Royales de Dissuasion)

Photo © Anthony Drugeon

Hisham Almiraat

Photo © Anthony Drugeon

Hisham Almiraat, médecin de formation, a cofondé la publication en ligne de citoyens reporters Mamfakinch en 2011 pour couvrir et soutenir le mouvement du 20 Février, une série de manifestations qui a eu lieu au Maroc à l'époque du Printemps arabe.

Mamfakinch remporte le Google Breaking Borders Award en 2012. Cette année-là, les quinze membres de la rédaction sont visés par un logiciel espion conçu par la société de surveillance italienne Hacking Team, qui permet à l'attaqueur d'obtenir un accès complet à l'ordinateur ciblé. Hacking Team commercialise ses logiciels espions uniquement à l'attention des forces de l'ordre et des services de renseignement, laissant peu de doute quant à l'identité de l'attaqueur.

Aujourd'hui, Hisham Almiraat est le président de l'Association des droits numériques (ADN). ADN est membre du réseau international des partenaires de Privacy International.

Hisham Almiraat fait partie de cette génération de Marocains qui ont développé leur conscience politique à la fin des années 90. Le précédent roi Hassan II – le père du roi actuel Mohammed VI – étant mourant, décida de relâcher son contrôle des médias afin de faciliter la transition à son fils. Les libertés d'opinion et d'expression – inclues dans la Constitution – furent pour la première fois respectées et de nouvelles publications se multipliaient. « Du jour au lendemain on avait au Maroc de l'investigation, on parlait de tabous religieux, moraux… », raconte Hisham, qui était alors étudiant en médecine à Paris.

Maria Moukrim, une journaliste de renom et rédactrice en chef de la publication « Febrayer » commença sa carrière durant cette période, en 1998. « On pouvait écrire sur tout ce qu'on voulait. Par exemple, j'ai sorti un dossier sur une grosse affaire de corruption. Je n'ai eu aucun problème à l'époque, aujourd'hui ce serait très différent. »

Mais alors que le nouveau roi Mohammed VI assoit son pouvoir, cette ère de liberté prend rapidement fin.

« Entre 2001 et 2003, il y a eu une sorte de régression progressive et systématique du champ médiatique jusqu'à ce qu'on arrive à ce qu'on a aujourd'hui, c'est-à-dire un champ médiatique soit sous le contrôle direct du régime soit dépendant économiquement. L'un dans l'autre les médias ne sont plus libres », décrit Hisham.

Accéder à des informations objectives devenant de plus en plus difficile, avec un paysage médiatique largement dominé par des publications liées au régime,

Hisham réalisa vite le potentiel d'Internet comme outil démocratique. « C'est l'invention la plus révolutionnaire depuis l'imprimerie parce que ça donne aux gens ordinaires la possibilité de s'exprimer et de s'engager politiquement. J'en suis viscéralement convaincu : si on l'utilise comme il faut, cela va vraiment changer les règles du jeu. C'est quelque chose qui peut encore faire tomber des régimes. »

Enthousiasmé par ces nouvelles opportunités, Hisham évolue rapidement du statut de « consommateur d'information » à celui d'acteur à part entière dans le paysage des citoyens reporters marocains.

« J'ai commencé à bloguer en 2007. Je trouvais ça génial parce que les gens parlaient en leur propre nom : il n'y avait pas d'étiquette, pas de financement derrière, pas de partis politiques. »

Mais l'enthousiasme insouciant pour Internet ne dura pas longtemps au Maroc. En 2008, Fouad Mourtada est emprisonné pour avoir créé une page Facebook satirique caricaturant le frère du roi. Mourtada, un informaticien prometteur, devint ainsi le premier « prisonnier Facebook ». Il fut en effet accusé de vol d'identité pour avoir créé cette page au nom du frère du roi. Avançant pour sa défense que la page ne pouvait prêter à confusion puisqu'il s'agissait clairement d'une caricature, il fut néanmoins condamné à trois ans de prison. Il obtint le pardon royal après 43 jours de prison.

Ce triste évènement eut toutefois un impact remarquable au Maroc. L'emprisonnement de Mourtada donna naissance à une véritable communauté de militants prêts à se lever pour défendre la liberté d'expression sur Internet. « La première campagne à laquelle j'ai participé, c'était 'Free Mourtada' [Libérez Moutarda]», raconte Hisham. « Cet épisode – et beaucoup d'autres qui vont suivre – va réunir une communauté qui n'aurait jamais pu se réunir autrement, si ce n'était pour Internet. »

C'est à cette époque que Hisham rejoint Global Voices, une communauté internationale de blogueurs, citoyens reporters et traducteurs de 167 pays, où chaque contributeur raconte l'actualité de son pays. Quatre ans plus tard, en 2012, Hisham deviendra le directeur du Programme liberté d'expression de Global Voices.

« Global Voices a été un énorme carrefour de personnes qui sont un peu des croyants de l'Internet. Ce sont des gens qui ont adopté Internet comme un outil d'engagement politique redoutable. »

Et si le rôle des réseaux sociaux dans le Printemps arabe est désormais un lieu commun, Hisham et ses homologues blogueurs n'étaient pas près d'imaginer ce qui les attendait.

« L'année 2011, bien sûr, nous a tous pris de court. Personne ne s'attendait à ça mais on était chanceux parce que, d'une certaine façon, on était prêt. Il y avait déjà des réseaux, des points d'informations, on se connaissait sur Twitter, on avait des abonnés à nos comptes, on était nous-mêmes abonnés aux comptes des autres, on parle anglais, on comprend l'anglais, on écrit en anglais… Je me souviens très bien que Global Voices a été l'une des premières plateformes qui a senti que quelque chose d'anormal était en train de se produire en Tunisie. »

Hisham avait suivi avec enthousiasme les évènements en Tunisie et en Egypte. Alors quand des manifestations s'annoncèrent au Maroc, il sut que c'était à son tour de jouer. « Un groupe d'activistes a annoncé des marches le 20 février. On connaissait du monde en Tunisie et en Egypte, ceux qui étaient sur le terrain, ou qui médiatisaient la révolution. On a appris à imiter leur méthode de diffusion : les hashtags, tout ce qui deviendra par la suite très populaire. On a fait la même chose, on a essayé d'aider le mouvement au Maroc.

Quelques jours avant le 20 février, Maghreb Arab Press, l'agence de presse officielle du pays, a commencé à publier des mensonges sur le mouvement. Ils disaient que la manifestation allait être annulée, que le mouvement avait reçu de l'argent de l'étranger, que c'était un mouvement d'homosexuels et d'athées. C'est ce qui m'a vraiment convaincu de fonder Mamfakinch le 17 février, trois jours avant les manifestations. Ça nous a mis la rage au ventre, et l'idée derrière Mamfakinch, c'était de créer une plateforme libre et sans censure. On n'était pas forcément objectif, parce qu'on a pris le parti du mouvement du 20 Février, on était pour la démocratie, la vraie, totale, radicale.

Au début, quand on a commencé, il y avait une trentaine de personnes derrière le projet et tous ne voulaient qu'une chose : participer, contribuer, écrire, faire du volontariat. On était plein d'énergie, tout le monde voulait contribuer parce qu'on sentait que le rapport de force avait vacillé en faveur de la démocratie. »

Mamfakinch – « on ne lâche rien » en arabe – commença à couvrir ce mouvement qui était ignoré dans les médias traditionnels, alors que des dizaines de milliers de personnes marchaient dans les rues de toutes les grandes villes marocaines chaque week-end. Mamfakinch fut consulté par un million de visiteurs durant les quatre premiers mois, un succès remarquable compte tenu qu'Internet demeure relativement peu développé au Maroc. Articles, vidéos, interviews, cartes, éditos… Mamfakinch devint rapidement une plateforme polyvalente en charge de relayer l'information sur le mouvement du 20 Février mais se transforma également en un espace de libre parole, où des sujets de toutes sortes étaient abordés : des affaires internationales aux trucs et astuces pour tenir un blog à jour.

Une année s'écoula et le mouvement du 20 Février s'affaiblissait peu à peu ; pour Mamfakinch, il devint de plus en plus difficile de conserver l'attention de

ses lecteurs. « On sentait qu'on n'intéressait pas grand monde parce que les gens avaient repris leur vie normale. Ils ne voulaient plus entendre parler de révolution parce qu'en Syrie ça commençait vraiment à devenir hideux, on voyait les premiers réfugiés arriver... Il y a aussi ce fatalisme politique dans le monde arabe en ce moment : tout le monde se dit 'entre la peste et le choléra, entre les islamistes d'un côté et les dictateurs de l'autre, je préfère rester chez moi et ne rien faire.' C'était difficile de garder la même popularité mais on a continué à appeler à des réformes radicales. »

Alors que la popularité de Mamfakinch, et donc son influence, baissait, une chose étrange se passa : ils commencèrent à être attaqués.

2012 fut en effet l'année où le site commença à être visé par des attaques DDoS (« Distributed Denial of Service », attaque par déni de service). Les attaques DDoS ont pour but de rendre indisponible un serveur en le submergeant de demandes. Pour un site Internet, c'est comme si des centaines de personnes tentaient en même temps de se connecter : le site ne peut pas répondre à toutes les demandes et cesse de fonctionner. Les attaques se déroulaient généralement lorsque Mamfakinch couvrait les quelques manifestations émanant du 20 Février qui continuaient à avoir lieu en 2012.

Quelques mois plus tard, Mamfakinch fut victime d'une attaque qui réduira au silence l'opposition vitale que le collectif incarnait.

Comme tout site, Mamfakinch avait une page Contact permettant aux lecteurs de contacter l'équipe éditoriale et de leur envoyer par exemple des renseignements sur des enquêtes à poursuivre. Le 13 juillet 2012, un email d'un certain « i_imane11@yahoo.com » fut envoyé via la page Contact avec pour objet le mot « Dénonciation ». L'email écrit en français leur disait :

> « Svp ne mentionnez pas mon nom ni rien du tout je ne veux pas d'embrouilles… » [sic].

Une pièce jointe intitulée "scandale(2)" accompagnait l'email.

Environ quinze membres de l'équipe de Mamfakinch reçurent cet email. Parmi eux, sept ouvrirent la pièce jointe, découvrant ainsi une page vide. Il ne fallut pas longtemps pour que l'administrateur systèmes de Mamfakinch comprenne que derrière le soi-disant scandale se cachait en fait un logiciel malveillant.

Hisham et son équipe décidèrent d'envoyer le logiciel à Citizen Lab. Citizen Lab est un laboratoire interdisciplinaire, basé à Toronto, qui étudie les relations entre les technologies de communication et d'information d'une part et la question des droits de l'homme et de la sécurité de l'autre. Une partie

importante de leur travail consiste précisément à identifier les logiciels espions et technologies de surveillance utilisés contre les activistes dans les pays aux régimes autoritaires.

L'équipe de Citizen Lab analysa le virus et finit par identifier sa signature : la même que celle du logiciel espion produit par la société italienne Hacking Team.

Le logiciel – qui selon certaines sources coûterait 200 000 euros – offre un accès à distance aux ordinateurs contaminés. Les attaqueurs peuvent ainsi avoir accès à tous les documents sur les ordinateurs, lire en direct tout ce que les utilisateurs tapent – y compris leurs mots de passe – ou ce qui apparaît à l'écran, faire des captures d'écran et même allumer la caméra de l'ordinateur sans que l'utilisateur ne s'en rende compte.

« Ça m'a beaucoup affecté. On a littéralement été violé, c'est un sentiment de viol parce qu'on construisait quelque chose pour aider d'autres personnes. On a essayé d'utiliser Internet d'une façon intelligente pour laisser ensuite la parole aux gens et ce qui a été fait est le viol d'une entreprise démocratique. »

Les personnes, dont les ordinateurs ont été infectés, les ont formatés pour effacer le logiciel espion. Toutes, sauf une qui décida de ne pas le faire. « Il n'y croyait pas, il se disait qu'il n'avait rien à cacher », explique Hisham. « Je pense qu'il y a un problème culturel qui est complexe... Il y a des gens qui sont difficiles à convaincre, surtout les militants à l'ancienne qui utilisent en réalité Internet plus qu'ils ne le pensent. Quand tu leur poses la question, ils te disent 'moi mon ordinateur je l'utilise une fois sur deux… Je ne mets rien d'important.' Ils ne se rendent pas compte qu'il y a des métadonnées, qu'ils se font localiser au bout d'un moment en répétant un certain schéma. Mais ils optent pour l'indifférence en se disant que si le gouvernement veut les avoir, il les aura. »

Hisham et son équipe décidèrent de répliquer en améliorant leurs propres pratiques de sécurité : « Pour la première fois on a réalisé qu'il fallait qu'on ait une politique de sécurité. J'ai élaboré un plan de sécurité interne et un formulaire à remplir par tout le monde. Ça consistait au final à construire un plan B pour tout le monde. 'Si jamais tu te fais infecter, voilà comment faire pour récupérer tes données et pour que le site ne soit pas mis en danger.' C'était douloureux pour moi de réaliser que personne ne s'y est intéressé. C'était trop lourd, parce qu'on demandait aux gens leur adresse physique, de donner leur mot de passe à quelqu'un de confiance au cas où ils se fassent arrêter... Cette notion de sécurité numérique est difficile à vendre. Le résultat, c'est que les gens développent un comportement d'évitement. Ils se désistent, ils trouvent des excuses pour ne plus travailler avec toi, ils vont participer de moins en moins parce que – on ne peut pas leur en vouloir – il y a des carrières en jeu. La plupart des gens utilisaient des pseudonymes parce qu'ils étaient ingénieurs, avocats, etc. donc ils avaient une réputation à défendre. »

Petit à petit, Mamfakinch a arrêté de publier et le site n'est plus actif depuis février 2014. Certains à Mamfakinch pensent qu'il s'agit de la conclusion logique d'une publication qui avait vocation à couvrir un mouvement désormais révolu. Mais selon Hisham, Hacking Team est le véritable responsable : « Ils ont empoisonné cette technologie magnifique qui nous permettait enfin de pouvoir nous exprimer sans avoir peur. On a tué ça. Les gens se disent 'les règles du jeu ont changé, je ne prends plus de risques.'

Je suis en colère et je crois que Hacking Team mérite qu'on leur colle un procès. D'abord parce qu'il y a eu violation de nos données personnelles et ensuite à cause du mal que ces entreprises sont en train de faire à Internet, cet outil extraordinaire. Ma peur c'est qu'Internet va être réduit à un outil médiocre, commercial qui ne sert qu'à faire de l'argent.

Ce qu'on voit aussi, c'est que ça a rendu l'enjeu et les risques énormes pour des gens 'ordinaires' - qui ne veulent pas de problèmes et qui ont beaucoup à perdre si jamais leur identité est révélée. Ils préfèrent ne pas utiliser Internet et je pense que c'est un énorme manque à gagner pour le camp démocrate dans ces pays-là.

Par contre, les gens qui n'ont rien à perdre comme les djihadistes de Daech ont adopté Internet. Moi c'est ma thèse : on a rendu Internet dangereux pour les gens qui ont des choses à perdre mais qui veulent quand même participer, contribuer aux débats publics tout en restant en retrait.

Les régimes répressifs ont compris qu'Internet n'est pas à laisser entre les mains de leurs citoyens. Ils ont réalisé que la censure c'est très voyant, et là on leur a offert sur la table le joujou magique qui permet d'instiller la peur et de pousser les gens à s'autocensurer. L'idée même que l'on puisse être surveillé fait que les gens choisissent eux-mêmes de se retirer. »

Methodology

Cet article a été rédigé en janvier 2015. Il est basé sur une interview d'Hisham Almiraat qui a eu lieu sur Skype le 13 janvier 2015. L'interview était en français.

Ci-dessous vous trouverez les liens vers les entreprises, les articles et les recherches mentionnés dans l'article, ainsi que des lectures que nous vous recommandons.

Mamfakinch

- https://www.mamfakinch.com/

Google Breaking Borders Award

- http://googlepublicpolicy.blogspot.co.uk/2012/07/breaking-borders-for-free-expression.html

Hacking Team

- http://www.hackingteam.it/index.php/about-us

Pour en savoir plus sur l'affaire Mourtada

- http://en.wikipedia.org/wiki/Fouad_Mourtada_affair (EN ANGLAIS)
- http://news.bbc.co.uk/1/hi/world/africa/7258950.stm (EN ANGLAIS)
- http://news.bbc.co.uk/1/hi/7304361.stm (EN ANGLAIS)

Samia Errazzouki

Photo © Anthony Drugeon

Fille de deux Marocains qui ont immigré aux Etats-Unis, Samia Errazzouki connaît bien le contexte politique et social du pays de ses parents. Désormais doctorante à l'université Georgetown à Washington, sa ville natale, Samia était en train d'écrire un mémoire sur le Maroc quand le mouvement du 20 Février débuta en 2011. Bien que ses parents l'aient prévenu que le gouvernement ne tolère pas les opposants, elle commence à couvrir les manifestations pour Mamfakinch de chez elle aux Etats-Unis et devient rapidement un membre à part entière de la rédaction.

Et lorsque l'équipe est visée par le logiciel espion de Hacking Team, elle réalise que, même à 6 000 km de l'autre côté de l'Atlantique, elle demeure exposée aux mesures répressives du régime.

« Je préparais ma licence et je faisais des recherches pour un mémoire sur l'économie politique du Maroc quand le mouvement du 20 Février a éclaté », raconte Samia. « Je me suis vraiment intéressée à ce qui se passait et je voulais m'impliquer parce que je croyais beaucoup à ce pour quoi ils se battaient. Je suis tombée sur ce site qui s'appelait Mamfakinch qui me paraissait être le seul média vraiment informé des évènements. »

Le premier article que Samia publia dans Mamfakinch fut justement ce mémoire. « Tout le monde pouvait proposer des articles alors je leur avais envoyé cet article universitaire sur le secteur privé au Maroc et ils l'ont beaucoup aimé. » Quelques mois plus tard, Hisham Almiraat la contacte pour lui demander si elle accepterait de rejoindre l'équipe : « Ils avaient besoin de quelqu'un qui puisse écrire en anglais et traduire des articles. J'ai commencé en décembre 2011. »

Samia commença ainsi à couvrir les manifestations depuis les Etats-Unis et réalisa que la distance géographique ne l'empêchait pas de devenir un membre à part entière de l'équipe. « C'était une structure libre et tout le monde était tout aussi impliqué. C'était utile d'avoir ce décalage horaire, ça me permettait de pouvoir couvrir des rassemblements qui parfois se déroulaient tard dans la nuit, quand le reste de la rédaction dormait. »

Le mouvement s'organisant largement sur les réseaux sociaux, il y avait beaucoup à écrire en observant simplement ce qui se déroulait sur Twitter et Facebook. « Surtout compte tenu de la situation des médias au Maroc, qui sont largement contrôlés par le gouvernement, Twitter et Facebook étaient essentiels pour obtenir des informations sur les manifestations quand aucune publication, site Internet ou journal n'écrivait quoi que ce soit. »

Si Samia appréciait ses nouvelles responsabilités de citoyenne reporter, elle

gardait néanmoins toujours à l'esprit qu'elles n'étaient pas sans risques, le risque premier étant d'être surveillé. « La surveillance, ce n'est pas quelque chose qui me surprend, c'est un danger auquel j'étais préparée, mes parents m'en avaient toujours parlé. Je connaissais ce risque quand je suis devenue militante et j'ai donc fait un choix éclairé quand j'ai commencé. »

Pour Samia, la surveillance n'a d'ailleurs jamais été un concept étranger : « Aux Etats-Unis, j'habite à 30 km du quartier général de la NSA », s'amuse-t-elle. Mais elle savait pourtant que les choses au Maroc seraient différentes.

« Tu réalises quand tu travailles dans un pays qui a un régime autoritaire – et qui a l'habitude d'enfermer les journalistes qui écrivent des choses que le gouvernement ne veut pas entendre – que tu t'exposes à toutes sortes d'oppressions. Mais en vivant aux Etats-Unis et en ayant la nationalité américaine, je me sentais privilégiée et je me disais que je pouvais en faire un peu plus que quelqu'un qui serait au Maroc. »

Ce sentiment de privilège allait pourtant rapidement disparaître. L'été après son arrivée à Mamfakinch, le site est visé par un logiciel espion de Hacking Team, évalué à 200 000 € : seul un gouvernement était en mesure d'investir de tels moyens pour surveiller un groupe de citoyens reporters. « Je m'attendais à ce degré de surveillance, surtout avec Mamfakinch qui n'avait pas de hiérarchie, et où beaucoup d'entre nous étaient anonymes. Je pense que le gouvernement était très curieux de découvrir qui était derrière ce collectif. »

Bien qu'elle était à plus de 6 000 km du gouvernement que ses parents avaient quitté, ses liens avec le mouvement du 20 Février la plaçait dans la ligne de mire du régime. Le logiciel espion de Hacking Team, lui, ne connaît pas les frontières.

« Les articles et les documents qui étaient envoyés à Mamfakinch nous étaient transmis à tous. On a reçu un email en français qui disait quelque chose comme 'j'ai une information importante qui devrait vous intéresser.' Je n'ai pas téléchargé la pièce jointe parce qu'à ce moment-là j'étais pressée et je n'avais pas le temps de le faire. Puis c'est rapidement devenu clair de quoi il s'agissait.

J'avais l'impression qu'à Washington, j'étais protégée du régime marocain mais cet évènement m'a prouvé le contraire. Peu importe où je suis, que j'ai un passeport américain ou pas, je pourrais être dans l'Antarctique, si le gouvernement marocain veut me garder à l'œil, il le fera.

Ça m'a rapprochée de mes collègues, ceux qui étaient au Maroc et en Europe. On s'est tous sentis autant visés. Il y a toujours une grande inquiétude pour ceux qui sont basés au Maroc. Nombre d'entre eux ont reçu des visites de la police ou savent qu'ils étaient suivis. »

Mais après Hacking Team, Samia découvrit que le régime avait d'autres

surprises désagréables pour elle et sa famille, restée au Maroc.

« Ma propre famille et mes voisins ont été visités par la police à plusieurs reprises. Ils venaient et demandaient : 'Est-ce qu'on peut vous parler quelques minutes ? Nous avons des questions à vous poser sur Samia et son travail.' La démarche de venir interroger ma famille et mes voisins, ce n'est pas pour obtenir des réponses ou des informations, c'est simplement pour m'intimider et me faire passer un message : 'On veut que vous sachiez qu'on vous surveille, pas seulement sur Internet mais dans la réalité aussi'. Le fait qu'ils interrogent le concierge ou mes voisins – qui n'ont aucune idée de ce que je fais – sur mon travail, ça me prouve qu'ils veulent juste m'intimider.

Une partie de ma famille est toujours ici au Maroc et après que la police les ait visités, ils m'ont mis une certaine forme de pression en me demandant ce que je faisais et d'y mettre un terme. »

Alors qu'elle se remémore ces évènements, Samia est assise à la terrasse d'un café à Rabat. Elle est au Maroc quelques jours pour voir sa famille, avant de les laisser derrière elle pour retourner aux Etats-Unis.

« On pense qu'on peut protéger sa famille de ce qu'on fait. Pourquoi est-ce que ma famille devrait être tenue responsable de mes actes ? Ils n'ont rien à voir avec ce que je fais ! Mais le gouvernement fait ça parce que c'est leur moyen de s'en prendre à moi psychologiquement. Ils augmentent le prix à payer parce que subitement je ne m'inquiète plus tellement pour moi – après tout, j'avais pris cette décision de m'engager en étant informée des risques que je courais personnellement – mais parce que je n'avais jamais imaginé que ceux que j'aime puissent être affectés. Tu commences à te demander 'mais que vont-ils faire à ma famille la prochaine fois ? C'est quoi la prochaine étape ?' »

Mais même après Mamfakinch, Samia a continué à écrire sur le Maroc et à s'engager. Et le régime est en partie responsable : « J'ai réalisé que ce que je faisais comptait et que le travail qu'on fait est important parce qu'il n'en aurait pas après nous si ce n'était pas le cas. Si Hacking Team m'a affectée d'une manière ou d'une autre, ça a eu un effet positif, ça m'a poussée à poursuivre ce que je faisais. »

Samia est pourtant très au courant de l'impact de ses choix politiques sur sa vie et plus particulièrement sur sa carrière universitaire. Ses recherches de doctorat portent en effet sur un chapitre controversé de l'histoire marocaine moderne et être surveillée la confronte à d'importants dilemmes. « J'ai la responsabilité de protéger l'identité et la sécurité des gens que j'interviewe pour mes recherches. Ainsi la moindre personne à laquelle je parle ici, je l'expose au risque d'être ciblée… Je peux prendre toutes les mesures du monde pour protéger mes communications mais ils pourront toujours décider de me suivre par exemple. Et s'ils me suivent et me voient entrer dans la maison d'une personne, qu'ils voient que je rencontre la personne, ça veut dire que j'expose cette personne à un

risque contre lequel je ne peux pas la protéger. »

Samia a discuté de son histoire avec des universitaires qui ont été confrontés à des dilemmes similaires et tous lui ont conseillé de mettre de côté son militantisme. Elle sait que si elle finit par s'y résoudre, ce sera au profit de ses recherches universitaires, pas parce qu'elle aurait cédé à des pressions politiques.

« Est-ce que c'est le moment où je dois commencer à remettre en question ce que je fais ? Je n'en suis pas encore convaincue, je crois que je peux encore tenter de réussir ma carrière universitaire tout en continuant à militer. Je ne suis pas encore prête à abandonner. »

Méthodologie

Cet article a été rédigé en janvier 2015. Il est basé sur une interview de Samia Errazzouki qui a eu lieu à Rabat le 12 décembre 2014. L'interview était en anglais et a été traduite en français.

A lire : l'article de Samia sur le secteur privé au Maroc

- https://www.mamfakinch.com/morocco's-political-private-sector/ (EN ANGLAIS)

Photo © Anthony Drugeon

Yassir Kazar

Photo © Anthony Drugeon

Yassir Kazar était chef du personnel dans une société de services en ingénierie informatique et enseignant en informatique décisionnelle à l'université Paris Descartes quand le mouvement du 20 Février débuta. Il rejoint Mamfakinch sans savoir alors à quel point cette décision changerait le cours de son existence : choqué par l'utilisation du logiciel espion de Hacking Team contre le collectif, il quittera son travail pour lancer sa société en sécurité informatique.

Yassir Kazar vivait à Paris et travaillait comme professeur en informatique décisionnelle (« business intelligence ») lorsque le Printemps arabe éclata. « C'était assez marrant parce que quelques mois avant que ça ne bascule, j'avais écrit un de mes premiers articles sur un journaliste tunisien qui avait été arrêté, Taoufik Ben Brik », raconte Yassir. « En me mettant à lire des auteurs comme Chomsky, j'ai réalisé qu'il y avait pas mal de gens qui critiquaient leur propre pays et je me suis dit que c'était un peu facile de critiquer les autres pays et qu'il fallait que je commence à regarder ce qui se passe chez moi. J'ai écrit mon premier article sur le Maroc en septembre 2010 et quelques mois plus tard il y avait le Printemps arabe. Du coup j'étais prédisposé à rejoindre un collectif comme Mamfakinch qui voulait écrire sur ces sujets. »

Quand les manifestations du mouvement du 20 Février ont débuté, Yassir décida qu'il ne voulait pas vivre ces évènements devant sa télévision et réserva à la dernière minute un vol pour Casablanca. Il racontait son vécu sur sa page Facebook et c'est là qu'il fut pour la première fois confronté à la méfiance de ses proches : « Mes potes me disaient 'mais pourquoi tu fais ca ? Mais n'importe quoi ! La patrie, tu es un traître...' Ça faisait déjà partie d'un engrenage malsain qui s'était mis en place : après tout on demandait pas des trucs délirants ! »

Peu après les premières manifestations, Yassir rencontre l'équipe de Mamfakinch et rejoint la rédaction à ses débuts. Un an après, un évènement allait bouleverser le reste de sa vie.

« On avait un formulaire de contact sur lequel on recevait régulièrement des informations de gens, des propositions d'articles ou des messages d'encouragement. Une fois on a reçu un message avec une pièce jointe intitulée « scandale » et la personne disait quelque comme 'surtout ne me mentionnez pas, je veux pas qu'on me reconnaisse' : il s'est avéré que tout était bien entendu bidon. Il y avait un document '.doc' en pièce jointe. J'ai vu le mail et je ne l'ai pas ouvert parce que j'avais l'habitude d'utiliser Google Drive pour ça, étant de nature assez paranoïaque. Les premières personnes qui ont ouvert ont commencé à dire 'c'est bizarre, le document est vide'. Là on a eu toutes les alertes rouges dans nos têtes et on a envoyé des messages en disant aux gens

qui ne l'avaient pas encore ouvert de ne surtout pas l'ouvrir.

Entre-temps on a transféré le message à des experts en sécurité pour qu'ils fassent le diagnostic et nous disent ce qu'ils avaient trouvé. Et là, ils ont dit qu'il y avait bien un logiciel espion de Hacking Team avec un enregistreur de frappe et la possibilité d'allumer la caméra. On a compris qu'on était dans quelque chose de ciblé, ce n'était pas le virus qu'on attrape par hasard. »

L'attaque prit Mamfakinch par surprise. Personne n'avait alors entendu parler de Hacking Team. Ceux qui avaient été infectés cherchaient des réponses à leurs questions et l'équipe éditoriale tout entière commença à réfléchir à une stratégie de sécurité informatique.

« Il y a toujours une différence entre une histoire qu'on te raconte, que tu vois à la télé ou que tu lis dans un journal et ce qu'on vit réellement. C'est un peu comme une agression, on peut te raconter, tu peux avoir de l'empathie pour la victime mais quand tu vis la chose, c'est traumatisant. Après on réagit tous différemment au traumatisme, il y en a qui arrivent à transformer ça en expérience positive et il y en a qui restent bloqués, surtout s'ils n'étaient pas encore à l'aise sur les questions de technologie. Je pense que certains membres se sont pris une vraie claque. »

Si Hacking Team était une surprise, ce n'était pas pour autant la première fois que Yassir était confronté à la surveillance de l'Etat. Quelques mois avant de recevoir l'email porteur du logiciel espion, son voisin avait été visité par la police qui l'avait questionné sur les habitudes de Yassir, s'il consommait de l'alcool, s'il allait à la mosquée.

« C'était déjà pas évident parce que tu te rends compte que tu n'es pas seul dans la vie et que les plus touchés par ce que tu fais peuvent être tes amis, tes connaissances… On peut les perturber. »

Yassir était surpris et choqué de découvrir que le gouvernement était prêt à investir

200 000 € pour qu'un logiciel espion vise Mamfakinch. Pourtant, et comme beaucoup au sein de Mamfakinch, il a aussi vu le côté positif de cette révélation : si le gouvernement avait dépensé autant, c'était bien que leur travail dérangeait et avait de l'importance.

« Cet instant-là a vraiment changé ma vie. Je me suis dit que la sécurité informatique c'est un vrai sujet aujourd'hui. Si j'ai monté ma boîte c'est pour ça, je me suis dit 'là oui, il y a un vrai souci, il y a quelque chose d'important qui se joue. On n'est plus du tout dans une démarche criminelle classique où on a juste à installer un anti-virus. On est sur quelque chose qui devient une

vraie problématique de société, où on peut cibler des individus, on te cible, on t'envoie un truc qui va scanner tes données, les remonter, etc ' On est en plein dedans et soit on décide d'affronter ça et d'apprendre à se débrouiller au mieux, soit ça peut être très traumatisant : ça peut modifier l'expérience d'Internet radicalement. »

Mais avoir fait partie d'un groupe visé par un tel logiciel espion a aussi laissé place à un vrai questionnement autour des questions d'éthique journalistique.

« S'ils veulent m'arrêter, ils trouveront toujours une bonne raison pour le faire, alors au

moins ce que j'écris doit être irréprochable d'un point de vue honnêteté intellectuelle. Se faire arrêter pour un article mauvais ou diffamant, ce serait dramatique. »

Aujourd'hui, avec sa société DefenseLab, Yassir forme à la sécurité informatique pour que chacun apprenne à devenir plus prudent et à protéger son entourage. Il demeure un militant de l' « open data », réclamant la transparence à l'échelle des gouvernements et défendant le droit à l'information. Faciliter le partage de l'information tout en protégeant les sources est un défi qu'il a justement découvert aux côtés de Mamfakinch.

« La question de la protection des sources s'est posée très clairement. Elle s'est posée d'autant plus qu'il y a des membres anonymes au sein de Mamfakinch et on a des échanges avec des sources extérieures. Parce que moi j'assume ce que je fais mais si mes bêtises permettent de remonter à quelqu'un qui a envoyé un document et qu'il se prend perpète, je vis comment, moi, avec ça ? Je vais sortir dans la rue parler de la justice et dire que c'est pas bien ? Non, bien sûr, ce serait un drame ! »

Méthodologie

Cet article a été rédigé en janvier 2015. Il est basé sur une interview de Yassir Kazar qui a eu lieu à Rabat le 13 décembre 2014. L'interview était en français.

Ali Anouzla

Photo © Anthony Drugeon

Si vous prononcez le nom d'Ali Anouzla au Maroc, vous ne laisserez sûrement pas votre interlocuteur indifférent. Bien connu du public et honni des puissants, Ali est un célèbre journaliste d'investigation et le rédacteur en chef de la publication en ligne «Lakome». Malgré des pressions de la part de diplomates marocains qui s'y opposaient, il remporte en 2013 le prix « Leader de la démocratie » de l'organisation Project on Middle East Democracy. En 2014, il est sélectionné par Reporters Sans Frontières pour faire partie de la campagne « Information Heroes ». «Lakome» est aujourd'hui inactif et ce depuis que le site a été bloqué par le gouvernement en octobre 2013. Il demeure cependant accessible via des sites miroirs.

En septembre 2013, Ali publie un article sur Al Qaïda, contenant un lien vers un article d' « El País », où figure une vidéo de l'organisation terroriste menaçant le Maroc. C'est cet article qui vaudra à Ali des poursuites pour « apologie du terrorisme », il est alors immédiatement envoyé en prison. Relâché cinq semaines plus tard, il est, encore aujourd'hui, en liberté conditionnelle, les accusations ayant été maintenues. Selon Ali, la raison réelle de ces poursuites est liée à un article de «Lakome» paru un mois auparavant qui avait vivement déplu au roi Mohammed VI. L'article dénonçait en effet un scandale politique impliquant la libération d'un pédophile espagnol, et les révélations avaient conduit à de violentes manifestations dans le pays. Les manifestations reflétaient la colère de groupes divers, des associations de protection de l'enfance aux organisations religieuses en passant par les groupes pro-démocratie, choqués par les dysfonctionnements du système juridique marocain.

Ali Anouzla raconte à Privacy International ses nombreuses expériences de surveillance, des écoutes téléphoniques aux piratages de ses comptes Facebook.

Alors que l'attention est aujourd'hui largement portée sur la question de la surveillance des communications électroniques, Ali Anouzla souhaite rappeler que l'on peut être une victime d'espionnage de toutes sortes. « Il y a des voitures qui m'ont suivi en dehors de Rabat, une personne est venue filmer le trou de ma serrure. Il s'est avéré qu'il travaillait pour les services secrets. Et bien évidemment les téléphones sont sur écoute. »

Ali a de nombreux récits d'écoute téléphonique. L'un d'entre eux concerne une sénatrice belge qui lui avait téléphoné pour lui dire qu'elle souhaitait le rencontrer pendant son voyage au Maroc. Les deux s'accordent sur un lieu et un horaire pour le rendez-vous et n'en parlent à personne. Peu de temps après,

la sénatrice reçoit un appel téléphonique du ministère marocain des Affaires Étrangères lui réclamant d'annuler son entretien. Bien qu'ils n'ont pas donné d'explications concernant la manière dont ils avaient eu connaissance de ce rendez-vous, un renseignement des services secrets suite à des écoutes téléphoniques semble être le plus plausible.

« Sincèrement, la surveillance n'a pas un grand impact sur ma vie professionnelle ni même sur ma vie privée », revendique Ali. « Mais c'est vrai que ça me dérange de savoir que je suis toujours sur écoute, sous contrôle, sous surveillance. Ça restreint ma liberté, surtout en ce qui concerne ma vie privée : par exemple je ne peux pas aller dans des lieux publics où je pourrais être pris en photo aux côtés de gens qui boivent, même si je suis quelqu'un qui ne boit pas, dans un pays conservateur où beaucoup de gens sont des musulmans pratiquants, ça pourrait être utilisé pour choquer les gens. Mais à part ça, ça n'a jamais affecté ma liberté d'expression. »

Au-delà des écoutes téléphoniques et des diverses attaques à sa vie privée, Ali a aussi découvert les ressorts d'un partenariat obscur entre certains médias en ligne et les services secrets.

« Parfois ces journaux publient des informations sur ma vie privée qu'ils ne pourraient avoir eues qu'en interceptant mes conversations téléphoniques, lorsqu'ils parlent de mes voyages, de mes fréquentations, de mes contacts… Une fois quelqu'un m'a appelé pour m'inviter à une conférence dans un pays étranger et le lendemain l'info sortait sur ce site alors que je n'en avais parlé à personne. »

Au Maroc, on dit qu'il y a trois sujets tabous : le roi, la religion et le Sahara occidental. La région est revendiquée depuis 1963 à la fois par le Maroc et le Polisario, le mouvement d'indépendance sahraoui. Le Maroc réclame d'une part l'appartenance de la région au royaume, tandis que le Polisario – un mouvement républicain – réclame l'indépendance et la souveraineté totale du Sahara occidental. Au Maroc, remettre en question – comme le fait Ali Anouzla – la position du royaume sur le Sahara occidental peut être lourd de conséquences.

En avril 2013, plusieurs de ces médias en ligne qui publient régulièrement des articles issus d'écoutes téléphoniques, annoncèrent au milieu de la nuit qu'Ali Anouzla s'était suicidé, suite à une résolution des Nations Unies favorable au Maroc sur la question du Sahara occidental.

« Ça a eu beaucoup d'impact sur ma famille, mes amis… J'ai passé la nuit à répondre à des appels pour leur dire que j'étais sain et sauf. Je n'ai pas attaqué ces sites parce que j'ai déjà l'expérience de l'avoir tenté et rien ne se passe.

Le lendemain, des journalistes amis m'ont demandé ce qui se passait. Je leur ai dit que je n'allais pas répondre à des sites manipulés par les services secrets. Certains sites ont relayé ces propos : « Ali Anouzla déclare que ces sites sont manipulés par les services secrets», le ministère de l'Intérieur a alors publié un communiqué pour dire qu'aucun site n'était manipulé par les services secrets et une semaine après, j'avais un procès en diffamation. »

La cour a d'abord rejeté la plainte du ministère. Le ministère a fait appel et Ali a été condamné à une peine d'un mois de prison avec sursis. Pourtant Ali n'ayant jamais été prévenu que l'audition avait lieu, il n'était donc pas présent – et il fait à ce titre appel de la décision.

« Il faut voir le paradoxe : quand j'attaque ces sites qui s'en prennent à ma vie privée, ils sont acquittés et ma requête est rejetée par le tribunal et quand je dis qu'ils roulent pour les services secrets, je suis attaqué par le ministère ! »

Les violations de la vie privée et la surveillance ne sont d'ailleurs pas seulement le fait des forces de l'ordre marocaines. Plusieurs collectifs de hackers sont connus pour s'en être pris à des militants et des journalistes critiques à l'égard du régime. Ces groupes se font appeler les Jeunesses monarchistes, la Force de répression marocaine et le Groupe nationaliste marocain. Leurs « victoires » sont célébrées dans les médias qu'Ali soupçonne d'être liés aux services secrets.

Les groupes de hackers marocains sont connus sur Internet pour viser tout ce qu'ils jugent « antipatriotique » et trahissant les valeurs traditionnelles du royaume. Leurs cibles sont souvent hétéroclites, les sites algériens et israéliens sont souvent visés mais la Française des Jeux compte aussi parmi leurs victimes. Cette dernière a été attaquée par un groupe connu sous le nom de Moroccan Ghosts, qui avait alors affiché un message rappelant aux croyants que les jeux de hasard étaient impies.

Une autre figure bien connue du journalisme indépendant marocain, qui a préféré garder l'anonymat, nous raconte comment son ordinateur a été infectée par un virus après qu'elle ait cliqué sur un lien qui lui avait été envoyé par la Force de répression marocaine. Elle découvrit

ensuite que ce virus leur permettait d'allumer la caméra de son ordinateur afin de prendre des photos d'elle.

En ce qui concerne Ali, ce sont ses comptes en ligne qui furent visés.

« Mes comptes Facebook et Gmail ont tous les deux étaient piratés. C'est un peu de ma faute, j'avais fait l'erreur d'utiliser le même mot de passe pour tous mes comptes. Je n'ai jamais pu récupérer les comptes. Après les piratages de mes comptes, un site d'information proche des services secrets a révélé que

la Brigade royale de dissuasion, un groupe dans la mouvance des Jeunesses Monarchistes, avait annoncé avoir réussi avec succès à pirater mon compte Facebook et avait attaqué des sites algériens et celui du Polisario. Pour eux, c'est un acte héroïque de nationalisme. Ils considèrent que quelqu'un qui a des points de vue indépendants de ceux de l'Etat sur la question du Sahara, c'est quelqu'un qui a des positions pro-Polisario. »

La publication en ligne «Chaabpress» avait en effet publié un communiqué de presse de la Brigade royale de dissuasion, où Ali est désigné comme « le porte-parole officiel d'un mouvement douteux » (le mouvement en question étant celui du 20 Février) et où le groupe de hackers menace le reste de la rédaction de « Lakome » : « Ceci est un avertissement à toute la rédaction de 'Lakome' : sachez que pirater votre site nous est facile mais parce que – contrairement à vous – nous croyons en la liberté d'expression, nous préférons ne pas vous porter préjudice puisque vous êtes aussi Marocains. Mais soyez certains qu'au cas où vous dépasseriez les limites, vous goûterez à notre colère. »

Selon Ahmed Benseddik, un célèbre militant notoire que nous avons interviewé à Rabat, la police est réticente à arrêter ces groupes. Il a ainsi déposé une plainte contre les Jeunesses monarchistes qui avaient posté une vidéo sur YouTube, où ils appelaient à son assassinat ainsi qu'au meurtre de neuf autres journalistes et militants. La police n'a pas donné suite à cette affaire depuis juin 2014.

Ahmed Benseddik a lui aussi vu ses comptes piratés et le contenu de ses emails publiés. Il mentionne par exemple un email ironique qu'il avait envoyé à une journaliste que les hackers ont utilisé pour avancer qu'il aurait eu une liaison avec elle. « Leur but est de nuire à la réputation de la personne et d'essayer de détruire le foyer par des méthodes sales et immorales », constate Ahmed Benseddik.

Mettre la lumière sur les motivations réelles de ces groupes – et ceux qui se cachent derrière eux – sera désormais le travail des journalistes d'investigation et des militants marocains.

« En tant que journaliste, je ne peux pas me prononcer et dire que ces groupes sont directement liés aux services secrets parce que je n'ai pas de preuves mais j'ai des soupçons », explique Ali Anouzla. « Avant mon emprisonnement, nous étions en train de travailler sur ces groupes. Malheureusement nous n'avons pas pu terminer cette enquête mais on la reprendra un jour. »

Methodology

Cet article a été rédigé en février 2015. Il est basé sur deux interviews d'Ali Anouzla qui ont eu lieu à Rabat le 29 août et le 13 décembre 2014. Il contient aussi des extraits d'interviews avec Ahmed Benseddik et Maria Moukrim qui ont eu lieu respectivement les 28 et 29 août 2014 à Rabat. Les interviews étaient en français.

Ci-dessous vous trouverez les liens vers les articles et les recherches mentionnés dans l'article, ainsi que des lectures que nous vous recommandons.

Pour en savoir plus sur les manifestations qui ont suivi le pardon royal d'un pédophile espagnol

- http://www.theguardian.com/world/2013/aug/04/dozens-injured-morocco-protest-spanish-paedophile
- http://uk.reuters.com/article/2013/08/03/uk-morrocco-spain-protest-idUKBRE97202520130803

L'article de Chaabpress contenant le communiqué de presse de la Brigade Royale de Dissuasion

- http://chaabpress.com/news4466.html

Privacy International veulent remercier Antony Drugeon pour les photos présentées dans ce compte rendu.

Photo © Anthony Drugeon

Photo © Anthony Drugeon

PRIVACY INTERNATIONAL

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471