Version condensée de l'entretien. Les parties en italique ne sont pas des propos énoncés, mais un résumé de ce qui a été dit. J'ai conservé ces parties à la première personne pour ne pas gêner la lecture, mais ce ne sont pas les propos directs d'Amadine Jambert.

Vincent Jarasse : Bonjour Amandine Jambert. Tout d'abord, quel est votre rôle au sein de la CNIL ?

Amandine Jambert : Initialement je suis cryptologue, j'ai une thèse en cryptologie, et ici (à la CNIL) je travaille dans la protection de la vie privée. J'ai aussi des liens en dehors de la CNIL avec des associations de TOR.

VJ : La CNIL a été créée en 1978 après le projet SAFARI qui consistait à faire du fichage des citoyens. Maintenant que la loi sur le renseignement est passée, et que les boîtes noires ont été implantées, quels sont les liens entre la CNIL et le réseau TOR ?

AJ : La CNIL est une autorité administrative indépendante qui a une loi en gardiennage qui est la loi informatique et liberté. On protège la vie privée des gens, même un peu plus et un peu moins. Un peu plus en effet car au delà de la vie privée, cela peut être la liberté d'aller et venir, la liberté d'expression etc. à partir du moment où on est dans le cadre de cette loi. *Un peu moins car dès lors que cela ne touche plus aux données à caractères personnels d'un individu, ou que l'on est plus dans le cadre de cette loi, nous ne pouvons rien faire.* Notre mission est d'assurer le respect de cette loi : c'est une mission éminemment juridique. *On n'est donc pas forcément dans ce qui est éthique, où ce que l'on aimerait dire, mais nous pouvons donner notre avis à tire informatif. Concernant TOR, nous essayons de rester technologiquement neutres : un outil n'est pas par défaut bon ou mauvais, la question réside en la manière dont il est utilisé.*

VJ : En effet c'est là tout un pan de la controverse autour de TOR : créé avec de bonnes intentions, certaines personnes l'utilisent à des fins criminelles. Cependant on a l'impression que les médias n'en font ressortir que le côté sulfureux, si bien que la police souhaiterait fermer TOR, malgré les chercheurs qui affirment que ce n'est pas l'outil qui est défectueux.

AJ : Concernant le fait que la police souhaite fermer TOR, disons que j'en doute. Juste après les attentats, il y a eu une fuite d'une liste de « rêves » disons, de certains policiers. Parmi ces rêves, il y avait l'interdiction du chiffrement, l'interdiction du WIFI public et la fermeture de TOR. Ce n'était pas la wishlist du ministère de l'intérieur.
Un autre point intéressant est qu'à la base, le réseau TOR a été développé pour les services de police et d'enquête, des différents pays. Effectivement il y a une partie des utilisateurs constituée de journalistes et d'activistes de pays dictatoriaux, mais il y a aussi tout ce côté police. Ce n'est pas un secret de polichinelle que notre police, gendarmerie, DCRI et DCRE l'utilise et c'est normal, surtout que l'utilisation est licite en France : on ne peut pas arrêter quelqu'un en France pour l'utilisation de TOR. Le point de vue de l'association « nos oignons » est un peu différent car ils fournissent

des nœuds de sortie. Même si la fourniture de sortie n'est pas interdite en France, il peut y avoir des cas où il y a du contenu illicite qui en sort.

VJ : Concernant le lycéen de Dijon qui a été mis en garde à vue car il était suspecté de posséder un relai TOR par lequel avaient transité les fausses alertes à la bombe des lycées parisiens, n'est-ce pas surprenant que la police l'ait mis en garde à vue alors que juridiquement il n'y avait rien d'illégal ?

AJ : Le problème n'était pas le fait qu'il possède un relai TOR, mais plutôt est-ce qu'il a des logs ou pas, et qu'est-ce qu'ils contiennent. La police, qui était en pleine enquête, essayait de comprendre ce qu'il se passait, et a sans doute aussi compté sur le fait qu'en tant que lycéen, il devait être plus facilement impressionnable. Ils se sont alors retrouvé dans une situation où la seule peine appropriée est le refus de livrer des clés de chiffrement aux autorités. En réalité il y a très très peu de risques. L'association nos oignons existe maintenant depuis plus de 2 ans, et ils sont encore là !

VJ : Est-ce que l'on peut techniquement bloquer TOR ? Selon la presse, la Chine l'aurait fait, et pourtant la NSA essaierait en vain depuis des années…

AJ : La question c'est combien de temps. Il y a un principe de base de TOR, mais il y a énormément d'innovations en continu. Donc même si la Chine arrive à bloquer TOR à un instant t, à l'instant t+dt des évolutions auront été apportées pour contourner ce blocage. Mais en réalité la Chine ne ferme pas TOR. Ce qu'elle fait c'est faire en sorte que ça ne passe pas le firewall chinois. En soi on pourrait très bien faire fonctionner TOR au sein de la Chine, mais l'intérêt est limité. Concernant le blocage, comme je l'ai dit, les développeurs du projet TOR s'adaptent. A quoi reconnaît-on que du flux sortant d'un serveur est du flux TOR ? En fait il y a une empreinte propre au code TOR. Lorsque cette empreinte est identifiée comme du code TOR, il « suffit » de modifier cette empreinte pour être de nouveau indétectable. Concernant la NSA et TOR, je ne suis pas d'accord : les Etats-Unis ne cherchent pas à fermer TOR. S'ils cherchaient à fermer TOR, ils arrêteraient de le financer.

VJ : En effet actuellement 80% du financement de TOR provient des USA, part que les membres du projet TOR veulent diminuer à hauteur de 50%. Ce financement vient en contradiction de ce que l'on peut lire dans la presse concernant la NSA et TOR.

AJ : Tout à fait. C'est pourquoi les USA ne veulent pas fermer TOR, ils veulent l'utiliser. Malheureusement, ce qu'ils voudraient c'est pouvoir l'utiliser en attaque et en défense. Ils souhaiteraient pouvoir l'utiliser pour se protéger eux, leurs sources et leurs agents, mais s'ils pouvaient avoir une backdoor cela les arrangerait bien. Or aujourd'hui il y a pas mal d'indices qui laissent supposer qu'ils n'en ont pas. Eventuellement un jour ils interdiront l'usage de TOR sans avoir un permis, mais le fermer complètement cela semble très peu probable à partir du moment où ils l'utilisent.

VJ : Pourquoi y a t'il autant de controverses autour de TOR, notamment lorsqu'il est question de chiffrement, alors qu'il existe beaucoup d'autres outils de chiffrement que les personnes mal intentionnées pourront utiliser de toute manière si TOR venait à fermer ? Est-ce une mauvaise compréhension de l'outil ?

AJ : Je pense que la première raison réside dans les sites en «.onion ». Dans ce groupe, il y a un pourcentage non négligeable de sites qui présentent des produits illicites dans à peu près le monde entier. Le deuxième point est sans doute juste un problème de gestion d'image. C'est un outil qui permet de pousser l'anonymat le plus loin possible. Or en France nous avons des élus qui pensent que le pseudonymat – c'est à dire utiliser internet avec un pseudonyme et non avec nos vrais noms – c'est mal. On est donc là de l'autre côté du spectre, qui s'oppose à la vision de TOR, où tant que l'utilisateur ne dévoile pas son identité on ne saura jamais de qui il s'agit. Lorsqu'on regarde courbes d'utilisation de TOR, il y a deux groupes. Le premier est formé de pays comme la France ou les USA, ou il n'y a aucun problème, on est pas sous dictature, et on peut dire presque tout ce que l'on pense. L'autre groupe est quant à lui formé des pays les plus dictatoriaux. *Pour le premier groupe, auquel on appartient, TOR est quelque chose d'un peu obscur et compliqué, avec des gérants un peu atypiques. Lorsqu'on y ajoute les sites en .onion et les attentats, cela ne joue pas en faveur de l'image de TOR.*

VJ : Concernant les courbes d'utilisation de TOR, notamment en France, on se rend compte qu'il y a un pic d'utilisation en août 2013, après les révélations de l'affaire Snowden qui datent du 6 juin 2013. Pourquoi cette latence de 2 mois, et pourquoi une baisse régulière de l'utilisation après ce mois d'août ?

AJ : Je n'ai pas de grande révélations sur ce point, mais j'ai l'impression qu'en France il y a eu une latence entre les gens qui étaient dans le milieu et qui ont suivi heure par heure ce qu'il se passait, et les reste de la population Française qui n'a réagi que plus tardivement en se rendant compte que quelque chose s'était passé.

VJ : Concernant les sites en «.onion », les chercheurs affirment que justement ils sont négligeables en proportion.

AJ : Selon les chiffres, le trafic de sortie de TOR est en effet relativement comparable à l'internet classique. Cependant depuis quelques temps ces chiffres sont noyés dans le flux du à l'utilisation de Facebook, qui a créé une version en « .onion » utilisée quotidiennement par plus de 2 millions d'utilisateurs.