

Les temps de la sécurité informatique :

une anthropologie du soin du protocole cryptographique OpenPGP

Résumé de la thèse de doctorat

Cette thèse en anthropologie sociale analyse les pratiques de soin autour du protocole cryptographique OpenPGP. OpenPGP est un protocole de chiffrement asymétrique utilisé principalement pour assurer la confidentialité du courrier électronique et authentifier des données numériques. Au cœur de nombreuses controverses depuis des années, notamment liées à son ancienneté et sa complexité d'usage, il est néanmoins toujours utilisé car difficilement remplaçable pour certaines tâches. Cette thèse analyse comment de nombreuses personnes agissent afin de faire durer dans le temps la sécurité que cherche à offrir ce protocole, ce qui implique non seulement de s'accommoder de l'héritage du passé, mais aussi de (p)réparer l'avenir.

Basée sur une étude ethnographique de plusieurs années auprès d'équipes de développement et de recherche, cette thèse analyse la production sociale de la sécurité informatique en l'analysant au prisme du temps. Plus précisément, elle questionne les trois dimensions temporelles de la sécurité informatique que sont la transformation, le rythme et la durée. Elle propose une réflexion sur le vieillissement des technologies du numérique et sur les pratiques de soin à court et long termes des normes de sécurité informatique.

Cette thèse s'insère dans les champs d'études des sciences et des techniques et de l'anthropologie de la sécurité auxquels elle contribue en proposant plusieurs notions novatrices. Tout d'abord, dans une perspective inspirée de l'anthropologie de la sécurité et en particulier des approches constructivistes de la sécurisation, l'analyse propose les notions de « processus d'(in)sécurisation » et de « projet-sécurité ». Les processus d'(in)sécurisation soulignent la constante oscillation entre sécurité et insécurité. Cela amène à considérer la sécurité informatique non pas en tant que pure propriété technique mais en tant que processus relationnel. La notion de « projet-sécurité » permet d'approfondir cette dimension en axant l'analyse autour de ce qui est fait au nom de la sécurité. La sécurité peut en effet être considérée comme un projet, un objectif vers lequel on tend, tout en sachant qu'il ne pourra jamais être atteint de manière définitive. Finalement, la thèse suggère également la notion de « résilience prospective » afin de rendre compte de la constante projection dans l'avenir qu'implique le travail de soin.

Cette approche constructiviste, processuelle et relationnelle de la sécurité est finalement renforcée par une perspective transversale inspirée des approches féministes des sciences et des techniques. En effet, ce travail propose de reconsidérer la manière dont on parle de sécurité informatique : plutôt que d'utiliser un champ lexical viril et guerrier pour parler de sécurité de

manière dichotomique, cette thèse l'appréhende à travers le vocabulaire du soin, de la collaboration et du compromis.

Après l'introduction (chapitre 1) et une section méthodologique (chapitre 2), le troisième chapitre présente différentes approches de la sécurité, tant du point de vue des personnes qui cherchent à la produire que des scientifiques qui décrivent leur travail. Suivent ensuite trois parties de chacune deux chapitres qui forment le cœur de l'analyse : la première analyse l'influence du temps en tant que facteur de transformation (première partie) et questionne le vieillissement des technologies numériques. La deuxième partie est tournée vers les rythmes de la sécurité, qu'il s'agisse de situations d'urgence ou de lentes négociations. La troisième partie est quant à elle tournée vers l'avenir et explore les durées de la sécurité. Une conclusion revient sur les différents apports et souligne cinq valeurs centrales analysées dans cette thèse : la collaboration, la compatibilité avec le passé, les opportunités de transformation, le soin, et le compromis.