Les puits de saumure seraient similaires à des puits conventionnels de pétrole et de gaz, dont la technologie est bien maîtrisée. Les traitements effectués sur la saumure, le méthane et le CO_2 ne seraient pas plus complexes que ceux menés dans les usines pétrochimiques, une autre industrie mature. Finalement, le forage et l'exploitation des puits de saumure ressembleraient beaucoup aux opérations pétrolières pratiquées depuis des décennies. Ils ne nécessiteraient pas, comme les gaz de schistes, l'envoi et l'élimination de fluides chargés en produits chimiques pour fracturer la roche et en extraire le gaz.

Le risque d'augmenter l'activité sismique serait très faible. Des recherches récentes montrent que l'injection de grandes quantités de fluides dans certaines formations géologiques – parfois entreprise pour éliminer les eaux usées – pourrait accroître la probabilité de tremblements de terre. Cependant, le dispositif que nous proposons fonctionne en circuit fermé : toute la saumure injectée est d'abord extraite du même réservoir. Ainsi, la pression moyenne n'augmente pas. L'accroissement du risque sismique serait même inférieur à celui résultant d'installations géothermiques classiques, où l'eau circule souvent dans des types de roches plus dures et plus susceptibles de déclencher des tremblements de terre.

Des investissements incontournables

Si l'exploitation du méthane et de l'énergie géothermique couvrirait les coûts d'exploitation, la construction du système coûterait cher. L'investissement pourrait être répercuté sur les contribuables, comme c'est souvent le cas pour les centrales électriques, ou se traduire par une augmentation du coût de l'électricité. Mais n'importe quel effort significatif pour réduire les émissions de CO_2 aurait le même effet – que ce soit la construction de milliers de fermes solaires ou éoliennes, ou celle de 200 réacteurs nucléaires pour remplacer les centrales électriques au charbon.

Nos calculs indiquent que le système devrait fonctionner, mais il reste à le tester sur le terrain. Des chercheurs des laboratoires Sandia et Lawrence Livermore (rattachés au Département de l'énergie américain) et de l'Université d'Édimbourg, en Écosse, conçoivent des moyens d'injecter du CO_2 dans la saumure et d'en extraire de l'énergie. Et deux entreprises, qui souhaitent rester anonymes, envisagent la construction d'un site pilote sur la côte du golfe.

Pour limiter le réchauffement climatique, il nous faut réduire les émissions de gaz à effet de serre le plus tôt possible. La côte du golfe, aux États-Unis, est l'endroit idéal pour un système combinant l'exploitation de la saumure et la séquestration de CO_2. La construction de dispositifs similaires ailleurs augmenterait d'autant l'impact sur les émissions mondiales. Il reste à identifier précisément d'autres sites favorables, susceptibles de se trouver partout où il y a des hydrocarbures, le paramètre critique étant la présence de méthane dans la saumure. On pourrait commencer par chercher en Chine et en Russie, qui ont des émissions croissantes de CO_2 et d'importants bassins pétroliers et gaziers. ■

Les activités criminelles laissent souvent des traces dans les ordinateurs, téléphones et autres appareils électroniques. Le recueil et l'analyse de ces indices sont devenus une part essentielle des enquêtes judiciaires.

Simson Garfinkel

LES TRACES NUMÉRIQUES DU CRIME

L'ESSENTIEL

- **Les experts en informatique judiciaire recherchent des éléments significatifs dans les mémoires de dispositifs électroniques variés : ordinateurs, téléphones portables, routeurs de réseaux, etc.**
- **Pour ce faire, ils ont développé des techniques élaborées, visant par exemple à reconstituer des fichiers partiellement effacés ou à détecter des photos retouchées.**
- **Les défis auxquels ils sont confrontés s'accroissent avec l'augmentation de la quantité de données et la diversification des matériels et des logiciels.**

Pour la Science, © Shutterstock/Igor Latsi

Depuis les années 1980, les ordinateurs sont de plus en plus présents dans la vie de tous les jours. Le monde du crime n'y échappe pas. Les criminels, comme d'autres personnes, stockent des données et communiquent avec leurs complices. Ces activités laissent des traces dans les appareils utilisés. Cela a conduit au développement de l'informatique judiciaire, qui vise à recueillir et à analyser les indices présents sur tout dispositif doté d'une mémoire numérique : ordinateur, téléphone portable, réseau...

Les experts de ce domaine sont confrontés à certains des problèmes les plus difficiles de l'informatique, tels que l'analyse de données massives et variées, le traitement automatique des langues naturelles et la cybersécurité. Ils sont impliqués dans l'élucidation de deux types de forfaits : ceux perpétrés dans le monde physique, mais dont des preuves sont enregistrées sur un dispositif électronique, et ceux qui sont intrinsèquement liés aux systèmes informatiques, tel le piratage. Nous examinerons ici la façon dont sont stockées les données sur un dispositif électronique, ainsi que les techniques développées par l'informatique judiciaire pour les extraire, les analyser, voire les reconstruire quand l'utilisateur a tenté de les effacer.

L'efficacité de l'informatique judiciaire vient de ce que nombre de systèmes numériques conservent de grandes quantités d'informations. Il s'agit d'examiner aussi bien les ordinateurs et les téléphones portables des suspects de crime que les données électroniques des entreprises lors de litiges. Les enquêteurs récupèrent souvent d'anciens courriers électroniques, des historiques de discussion en ligne, des termes de recherche sur *Google* ou d'autres types de données, créés des semaines, des mois, voire des années plus tôt. Ces enregistrements peuvent révéler l'état d'esprit d'un individu ou ses intentions au moment où un crime a été commis. Les techniques de l'informatique judiciaire peuvent aussi renseigner sur les victimes : un téléphone retrouvé sur un cadavre non identifié serait étudié de la même façon qu'un appareil perdu pendant un cambriolage.

L'informatisation rend l'enquête plus compliquée que si les données étaient inscrites sur du papier. Par exemple, Bernard Madoff, arrêté en 2008 pour des escroqueries financières, suivait les comptes de ses victimes sur un ordinateur IBM datant des années 1980. L'ancienneté de cette machine explique en partie la durée exceptionnellement longue de la fraude – qui a couru sur plus de deux décennies –, car peu de personnes à Wall Street maîtrisaient encore ce type de matériel. Elle a aussi compliqué l'interprétation des données après l'arrestation de B. Madoff.

Les indices numériques peuvent aussi révéler une absence de manipulation. En mai 2006, un ordinateur portable et un disque dur externe ont été dérobés au Département américain des anciens combattants. Ils contenaient des données sensibles concernant plus de 26 millions de vétérans et d'employés de l'armée. Quand l'ordinateur a été retrouvé en juin 2006, les enquêteurs ont montré que les dossiers sensibles n'avaient probablement pas été consultés. Pour ce faire, ils ont notamment examiné les heures d'accès et de modification associées à chaque fichier. Mais en utilisant les mêmes techniques judiciaires qu'eux, les coupables auraient pu visionner les fichiers sans modifier ces horodatages ; en fait, les enquêteurs ont juste déterminé que les fichiers n'avaient pas été ouverts par des moyens classiques.

Des données volatiles et invisibles

En pratique, les informations obtenues ne sont pas tant limitées par la technologie que par les coûts et les besoins. Le désir intellectuel d'examiner jusqu'au dernier octet est rarement justifié et l'on s'arrête souvent quand on en sait assez pour incriminer un suspect. Les contraintes légales conditionnent aussi la façon dont l'analyse est effectuée.

Les données électroniques nécessitent une attention particulière. Une mauvaise manipulation peut vite les modifier, les endommager ou les effacer. Le simple fait d'allumer un GPS du commerce risque d'entraîner la suppression de preuves cruciales. En outre, les ordinateurs contiennent souvent des informations cachées, pour lesquelles ont doit utiliser des outils spécifiques. Par exemple, un appareil photo qui semble contenir 30 photos peut en réalité en renfermer plusieurs centaines, censées être effacées mais en réalité récupérables. En effet, quand un appareil « efface » un fichier, il ne nettoie pas la mémoire, il note juste que l'espace est disponible ; le fichier n'est supprimé que lorsqu'un autre