acteurspublics

Cyberattaque du fisc : le débat sur la responsabilité au sein de l'État monte

Formation, absence de dialogue entre le politique et la technique, absence de sanction… Les critiques pleuvent à l'encontre de l'État, dans le tourbillon de la cyberattaque ayant frappé la direction générale des finances publiques.

David Amiel, ministre de l'Action et des Comptes publics, et Amélie Verdier, directrice générale des finances publiques.

La petite musique monte, et pas qu'au sein du cercle d'experts en cybersécurité : les cyberattaques contre le service public se multiplient, les données s'échappent, et les annonces se multiplient. Mais l'intrusion d'un cybermalfaiteur au sein des données fiscales, bastion protégé par une administration régalienne qui a failli à son devoir, a un goût de gravité différent. "*S'il doit y avoir un sursaut cyber, c'est maintenant*", relève un ancien cadre du numérique de l'État.

La question qui se pose est la suivante : quelle est la responsabilité de l'État, non seulement dans la cyberattaque survenue fin juin, mais aussi dans la multiplication de celles-ci ? Doit-on l'imputer aux politiques, dont la cyber, et plus largement le numérique, est parfois absente des considérations ? À l'administration, qui ne met pas suffisamment en œuvre les politiques de sécurité pourtant actées depuis quelques années ? Force est de constater que la question reste loin d'être

tranchée. Elle se révèle d'autant plus complexe qu'elle implique un temps long propre à l'administration : les responsables sont-ils, sinon, ceux qui ont failli à leur mission hier ?

"*Les autorités s'engagent sans penser à la sécurité informatique, car ça ne les engage en rien. Si ça plante, on passe à autre chose. Ceux qui vivent des trucs finissent par partir, passent à autre chose, et cela devient le problème du remplaçant*", s'agace Stéphane Dubreuil, ancien responsable de la sécurité des systèmes d'information (RSSI) au sein de Bercy. "*Il ne s'agit pas de réclamer des têtes par principe. Mais tant que les conséquences seront, encore demain, supportées par les administrés, dans leur vie personnelle et quotidienne, et non par les chefs, il n'y aura pas de "sursaut cyber"*, a justement rappelé Raphaël Marichez, ancien chef du Réseau interministériel de l'État, et ancien agent du RSSI à l'Intérieur, sur Linkedin. Une posture publiquement abondée par Patrice Latron, actuel préfet de la Réunion, preuve que le débat s'est déclenché à tous les niveaux.

Concernant la direction générale des finances publiques, un consensus se dessine autour de la chronologie de l'attaque. "*Le ministre Amiel parle d'investigations approfondies, mais réalisées seulement après la revendication par le hacker : là, il y a une faute morale de la personne collective qu'est l'État",* analyse une source. Concrètement, l'administration a vu le problème fin juin, mais n'en a pas tiré toutes les conséquences et n'a pas prolongé l'investigation. La question se pose alors : sans la revendication, qu'en serait-il ?

À qui la faute ?

La responsabilité de l'État en matière de cybersécurité semble désormais pleinement établie. Si la cyberattaque survenue au printemps à l'Agence nationale des titres sécurisés (ANTS) avait commencé d'entamer sérieusement la confiance envers la sécurité des données, ce nouvel assaut ne laisse plus aucun hasard. Le ver est dans le fruit depuis des années, selon plusieurs observateurs. "*Je pense que pour la majorité des responsables de la sécurité des systèmes d'information (RSSI) qui connaissent l'État, ce n'est pas une énorme surprise. Depuis de nombreuses années, on essaye d'éclairer les risques*", regrette Stéphane Dubreuil, ancien RSSI de Bercy.

Pour un autre interlocuteur, "*la responsabilité première incombe au politique. Depuis 10 ans, le dernier Premier ministre à s'être intéressé au sujet de la cyber, c'est Manuel Valls. Là est le fond du problème : dans les discours de politique générale depuis le gouvernement Philippe II, on ne parle plus du numérique*, détaille un ancien conseiller de l'Anssi, ayant accompli une dizaine d'années dans l'agence. *Le problème réside dans le fait que les politiques n'ont pas compris à quoi servait le numérique : pour eux, c'est un outil d'ingénieur, au service des applications, de la maintenance."*

L'informatique, cette "fonction support"

Un avis partagé par un ancien cadre du numérique de l'État, qui reconnaît de son côté que "*l'informatique chez les hauts fonctionnaires demeure une fonction support. Ils ne voient pas en quoi cela crée de la valeur, pour eux, c'est de l'intendance, ils ne s'y intéressent pas, mais font ce qui est nécessaire d'un point de vue réglementaire, c'est-à-dire désigner un RSSI, pour être dans les clous."*

L'absence d'une politique forte sur la cybersécurité en France est le fruit de plusieurs facteurs, découlant majoritairement d'une prise en compte trop peu assidue de ce sujet. Une séquence médiatique récente a particulièrement fait grincer des dents à la suite de la cyberattaque survenue à

la direction générale des finances publiques (DGFiP) : la ministre déléguée chargée de l'Intelligence artificielle et du Numérique, Anne Le Hénanff, a indiqué sur la plateforme X "*ne pas avoir la cybersécurité comme responsabilité dans son portefeuille de ministre, chaque ministre étant responsable de la cybersécurité de son ministère sous contrôle du Premier ministre*".

Cette déclaration laisse perplexe, alors même que la ministre présentait, en janvier dernier, la stratégie nationale de cybersécurité 2026-2030 à Bordeaux. " *La réaction de la ministre est dingue : elle explique ne pas être responsable de la cybersécurité, alors qu'elle est responsable du numérique. Elle acte un schisme, alors que la solution aujourd'hui, c'est vraiment d'aligner la sécurité numérique avec cette même politique publique,* s'agace un ancien cadre du numérique de l'État. *On ne peut plus confier la sécurité numérique uniquement aux informaticiens, ça fait une dizaine d'années que c'est le cas."* L'absence d'une gouvernance claire et efficace, qui avait déjà été pointée du doigt fin avril lors de l'affaire de l'Agence nationale des titres sécurisés (ANTS), rend impossible la définition d'une responsabilité concrète.

Mettre le RSSI dans les décisions

Le manque d'alignement des politiques liées au numérique se conjugue avec l'absence de reconnaissance des RSSI, ces responsables de la sécurité des systèmes d'information, garants de la sécurité numérique des infrastructures au sein de l'administration. Ce poste stratégique demeure, selon nos interlocuteurs, bien trop absent des préoccupations des directions générales. "*Le dialogue entre l'exécutif et le RSSI n'existe pas aujourd'hui : le RSSI est trop bas dans l'organigramme, comme on le voit dans celui de la DGFiP. S'il n'y a pas de dialogue entre le ministre et les gens sur le terrain, ça ne peut pas marcher"*, explique un ancien de l'État ayant passé plusieurs années à ce poste.

"*Les hauts fonctionnaires de l'État n'ont pas toujours une grande expérience. Il faudrait plus de reconnaissance pour les RSSI, qu'ils deviennent les interlocuteurs des directions centrales pour mieux anticiper, avoir un rôle plus important sur le budget*", relève Jean-Michel Mis, ancien député et vice-président du groupe d'études "cybersécurité et numérique » à l'Assemblée nationale, entre 2019 et 2022. Les conséquences d'une politique publique défaillante se font ressentir sur les outils de l'administration, qui demeurent défaillants à la fois sur la cyber et sur la protection des données. Une faute par ailleurs avouée par le ministre de l'Action et des comptes publics, David Amiel, qui a admis que les outils de détection d'intrusion dont dispose l'administration sont obsolètes.

"*Là se trouve aussi la responsabilité des dirigeants : se sont-ils intéressés au fait que l'organisation de la défense numérique était correctement établie, sans juste la reléguer au RSSI par principe ?*" des interrogations qui, par ailleurs, se renforcent à mesure que l'absence de sanctions effectives demeure au fil des assauts cyber subis par l'administration. Comme l'ont rappelé plusieurs députés, dont Jean-Luc Warsmann, à ce jour, aucun dirigeant d'agence publique, haut fonctionnaire ou responsable de système d'information n'a vu sa responsabilité personnelle, disciplinaire ou administrative engagée, y compris lorsqu'il est avéré que les mesures de prévention élémentaires avaient été négligées même après des alertes préalables. L'exécutif a, pour l'heure, partagé des excuses et garantit sa conscience de la gravité de la situation. Mais l'heure ne semble pas aux sanctions. "*Qui toucheraient-elles, de toute façon ?*", concède un proche du numérique de l'État. "*Les excuses ne suffiront plus*", relève un autre.

“*Le fond du sujet, c’est que s’il n’y a pas un poids qui s’exerce sur les épaules du chef, il ne peut pas y avoir une mise en œuvre efficace. Il faut que ceux qui sont tout en haut soient impliqués dans ces enjeux cyber*”, partage Stéphane Dubreuil, ancien RSSI de Bercy.

Conscientiser les enjeux

La responsabilité de l’administration auprès de ses agents est aussi en jeu : nombreux sont ceux qui mettent en doute la formation, en matière de cybersécurité ou simplement d’hygiène numérique basique, proposée aux agents. Se pose donc le problème de la formation, de la conscientisation des enjeux, de la sensibilisation : comment s’assurer que les personnes de l’État aient réellement conscience de ces enjeux ? L’une des annonces formulées par Amélie Verdier va en ce sens : la directrice générale des finances publiques a affirmé vouloir renforcer et améliorer l’offre de formation cyber à destination des agents de sa direction.

En définitive, la cyber n’est pas l’affaire que d’une direction obscure “*tout au fond du couloir à gauche*”, comme le rappelle l’un de nos interlocuteurs. “*On ne peut pas créer la confiance sur de la réponse à incident : ça doit se faire sur le temps long*”, rappelle Jean-Michel Mis. La crise cyber à la DGFiP, aussi grave soit-elle, sera peut-être le “sursaut cyber” attendu, nécessaire pour faire bouger les lignes.

“*Depuis le début de l’année, il y a eu une dizaine de fuites de données, et tout le monde s’en fout : elles n’ont aucun impact politique,* relève cet ancien cadre du numérique dans l’administration. *Aujourd’hui, ce qui se passe semble avoir un impact : l’opposition, les syndicats, le Sénat, les politiques montent au créneau. La vraie responsabilité, c’est peut-être d’être digne de ce moment.”*

Par Victoria Beurnez