LA RSE DANS UNE SOCIÉTÉ DE CYBERSÉCURITÉ :

QUELS CHOIX STRATÉGIQUES ET QUELLES CONSÉQUENCES ?

MARIE LE PARGNEUX
directrice des programmes dirigeants et potentiels du groupe BPCE

LAURENT OUDOT
cofondateur et directeur technique de TEHTRIS

Galvanisées par une hyperconnectivité, les cybermenaces se multiplient et ont un impact économique et sociétal croissant. En réaction, la demande de service explose, générant un marché énorme pour les firmes spécialisées, mais elle pose de nouveaux problèmes éthiques : la protection des données de l'entreprise donne du coup potentiellement accès pour des tiers à des données sensibles… le risque de faire entrer le loup dans la bergerie est réel.

Tehtris a été créée en 2010 par deux anciens de la DGSE, dont Laurent Oudot, *executive master* X 2018. Laurent a réalisé un projet d'équipe sur le développement très rapide de l'entreprise, qui est passée de 20 à 40 salariés au cours du premier semestre 2019. Marie Le Pargneux (*executive master* X 2018 et directrice des programmes dirigeants du groupe BPCE), spécialiste des questions de management, a contribué aux travaux de cette équipe. Ces deux camarades se livrent ici à un dialogue au croisement des questions de management et de « cybersécurité éthique », un nouveau champ d'exploration pour la RSE.

Marie Le Pargneux : Si je devais qualifier la principale spécificité du dirigeant aujourd'hui, je dirais que c'est avant tout un leader qui fait face à des tensions. Tensions entre un temps business court et une transformation culturelle longue, entre centralisation et décentralisation, entre pragmatisme et ruptures, entre autonomie et contrôle, etc., dans un contexte de profonds changements sociétaux, politiques et économiques. Au cœur de ces tensions, la RSE, souvent questionnée dans son lien avec la performance financière, n'est plus – ou ne devrait plus être – une activité connexe, dans un département dédié, mais devrait au contraire s'intégrer dans la réflexion business. Avec votre société, vous semblez avoir réfléchi dès sa création à l'impact de vos produits et de vos actions sur vos clients, et plus globalement sur la société. Que recouvre en fait cette idée de cybersécurité éthique ?

Laurent Oudot : La cybersécurité éthique est un concept encore émergent. On parle souvent de « hackers éthiques » et, dans le monde de la cybersécurité, la plupart des acteurs s'arrêtent là. Le « hacker malveillant » est un pirate informatique qui pénètre illégalement dans des systèmes. À l'opposé, au sens noble, un « hacker éthique » contribue techniquement à la sécurité, notamment *via*

REPÈRES

TEHTRIS est une entreprise experte en cybersécurité. Elle a créé la solution de cyberdéfense TEHTRIS XDR Platform, déployée dans de nombreux secteurs d'activité : industries, banques, assurances, supply chain, ingénierie, etc. Cette plate-forme globale, en mode security by design, 100 % française, offre une expertise technique de lutte contre le cyberespionnage et le cybersabotage, avec des experts opérationnels qui surveillent des infrastructures dans le monde entier. L'entreprise est devenue membre du club Microsoft Virus Initiative et son moteur d'intelligence artificielle scanne plus d'un million de fichiers par jour sur VirusTotal de Google.

des tests d'intrusion dans les systèmes informatiques afin d'y déceler des failles. Les défenseurs pourront alors protéger leurs infrastructures avant l'arrivée des véritables attaquants. Une cybersécurité éthique va selon moi au-delà. Elle passe par exemple par le souci de la confidentialité des données des entreprises clientes. Dans notre cas, nos systèmes de protection possèdent une couche de sécurité avancée, qui étanchéifie l'accès aux données sensibles du client. Curieusement, certains produits ajoutent des accès risqués vers les données des entreprises qui les adoptent. Nous refusons cette pratique, malgré la complexification que cela entraîne pour le développement technologique de nos solutions. Depuis la création de Tehtris en 2010, nous combinons toujours les concepts de *security by design* et de *privacy by design*.

M.L.P. : Mais du coup cela ne vous coûte-t-il pas plus cher en développement ? Et cela ne vous fait-il pas perdre des occasions de contrat par méconnaissance des données du client ? Ce serait un cas où RSE et performance économique ne vont pas ensemble…

L.O. : Oui et non… Nous avons pris des risques en combinant nos critères de sécurité et d'éthique, avec des développements initiaux plus importants et un retard potentiel sur certains marchés. Nous avions l'intuition en retour que, pour les clients capables de se projeter dans nos systèmes de valeurs et de qualité, nous aurions une reconnaissance technologique à rebours et une certaine fidélité, ce qui s'est confirmé. Néanmoins, dans certains cas, pour les entités qui acceptent une mise en danger en adoptant des produits de sécurité moins peaufinés ou sans ce niveau de respect, je reconnais que la performance économique est amoindrie. C'est le prix à payer quand on pense sur le long terme, à charge pour nous de mieux partager notre système de valeurs.

M.L.P. : Pour faire face à l'imprévisible en matière de cybersécurité, vous avez créé des robots logiciels défensifs, tels les *smart sensors* de l'industrie 4.0, combinés avec de l'intelligence artificielle et une automatisation à outrance. Or l'actualité entraîne des questionnements légitimes concernant l'impact des réseaux de neurones en matière d'éthique, compte tenu du risque de perte de contrôle par les humains. Quel positionnement éthique avez-vous concernant l'intelligence artificielle et ces robots logiciels défensifs automatiques ?

L.O. : Nous sommes très attentifs aux conséquences de nos actions. Quand un virus inconnu apparaît dans le monde, ces agents peuvent le neutraliser sans intervention humaine, par exemple pour lutter contre les demandes de rançons (*ransomware*). Dans certains cas assez rares, nos robots logiciels défensifs pourraient avoir à décider de détruire le travail infecté et non sauvegardé d'un humain. Les débats sur la robotique et l'éthique sont souvent liés, et la première des trois règles proposées par Asimov stipulait qu'un robot ne peut ni porter atteinte à un être humain, ni, en restant passif, permettre qu'un être humain soit exposé au danger. Ainsi, dans le cyberespace, s'organise la cohabitation entre les robots logiciels, l'intelligence artificielle et les activités humaines. C'est un point d'attention très fort pour nous et ces fonctionnalités sont couplées avec une sûreté paramétrable pour chaque client.

"La RSE n'est plus une activité annexe."

M.L.P. : On est en droit de se demander si, finalement, la cybersécurité éthique est une demande explicite des clients et un véritable avantage concurrentiel. *A priori*, aujourd'hui, pas encore suffisamment… Certes, la cybersécurité prend de plus en plus de place dans l'actualité. Je le vois dans différents secteurs d'activité, les dirigeants sont acculturés au risque encouru et se structurent pour y faire face, en termes de gouvernance, d'équipes, d'outils. Pour autant, quand on creuse, le marketing domine le marché et peu nombreux sont les clients qui s'interrogent sur la manière dont sont construits leurs systèmes de protection.

L.O. : En fait, le manque d'engouement de nos clients ne nous freine pas. Nous sommes convaincus de l'importance de notre engagement à déployer une cybersécurité éthique, en nous posant des questions à chaque innovation et à chaque nouveau développement informatique : comment respecter – vraiment – la confidentialité des données ? Ce que nous construisons permettra-t-il d'assurer l'intégrité des personnes et la continuité d'activité de nos clients en cas d'attaque, que ce soient des hôpitaux, des banques, des assurances, des producteurs ou distributeurs d'énergie, des industries, des services étatiques ? Comment assister nos clients, qui doivent informer les autorités et parties prenantes concernées qu'ils ont été attaqués, et quels seront les risques associés : une perte financière en Bourse en cas de communication mal maîtrisée, un impact négatif et durable sur l'image, etc. ? Cette dernière question s'est par exemple posée lorsque plusieurs multinationales ont déployé nos produits et que nous avons découvert qu'elles étaient espionnées depuis quelques années par des attaquants furtifs. Bien sûr – ne nous trompons pas – l'éthique est la « science de la morale », →

elle n'est pas coercitive et dépend d'un système de valeurs en profonde transformation. Adaptée au monde numérique, elle engage à de nouvelles réflexions et il nous faudra mieux la spécifier pour mieux agir et pour nous adapter. En vue de cela, nous étudions la mise en place d'un comité d'éthique de la cybersécurité.

M.L.P. : Cette vision nouvelle de la cybersécurité détermine en partie la gestion des équipes, ainsi que le modèle organisationnel et managérial de votre entreprise. Tehtris compte aujourd'hui plus de 40 salariés, son effectif a doublé en un semestre et devrait encore doubler dans les mois qui viennent. Vous avez décidé de ne pas définir de valeurs, contrairement à ce que font la plupart des organisations. La vision d'une cybersécurité éthique implique une responsabilisation forte des collaborateurs et donc des valeurs vécues plutôt qu'affichées. Le dialogue vaut mieux que la communication dans cet objectif.

L.O. : Oui, et c'est un travail de tous les instants, nous y consacrons énormément de temps.

M.L.P. : Mais alors, si en plus votre volonté est de conserver une organisation relativement plate, afin d'éviter le syndrome des « petits chefs » et la dilution des responsabilités, vous avez un sacré défi à relever. Ceux qui le souhaitent pourront demander à prendre un rôle annexe à leur activité. Petit à petit, certains pourraient devenir coordonnateurs planificateurs, d'autres, coachs techniques ou encore « développeurs de talents ». Déployer le « leadership responsable » envisagé n'est pas complètement naturel et simple car vos collaborateurs ont vécu un modèle éducatif très descendant et finalement assez hiérarchique. Ils peuvent aspirer à un autre modèle tout en manifestant parfois le besoin du confort d'un encadrement serré.

L.O. : Du point de vue de la gouvernance et du management, tout n'est pas abouti et, avec une équipe de plus en plus nombreuse qui se développe à l'international, de nouveaux challenges nous attendent. Pour terminer, notre démarche RSE ne serait pas complète si nous n'avions pas engagé des actions pour la protection de l'environnement, de manière plus « classique » peut-être. Nous avons choisi de nous installer dans un bâtiment écoresponsable, conçu pour minimiser l'impact sur l'environnement, au sein de la cité de la photonique de Pessac, certifiée ISO 14001, non loin du centre-ville bordelais. Nous nous engageons aux petits gestes du quotidien qui limitent la consommation d'énergie. À titre d'exemple, en 2018, les 18 salariés ont utilisé moins d'une ramette de papier d'impression [500 feuilles], nous visons une consommation maximale de trois feuilles par salarié et par mois. Nous avons également mis en place une politique d'achat responsable, avec la recherche de producteurs locaux ou de matériaux recyclés ou recyclables. Nous avons obtenu en janvier 2018 la reconnaissance au niveau *Silver* du classement EcoVadis CSR (*Corporate Social Responsibility*).

"Peu nombreux sont les clients qui s'interrogent sur leurs systèmes de protection."

M.L.P. : Avec la croissance, d'autres tensions et questions apparaîtront. Faudra-t-il choisir un jour entre développer de l'emploi et respecter certaines règles que nous qualifions d'éthiques dans la cybersécurité ? Entre maintenir les intérêts d'un État et protéger ceux de ses citoyens ? Comment « structurer sans rigidifier » une organisation en forte croissance ? Comment gérer les salariés, aujourd'hui très engagés pour la cybersécurité éthique et la démarche RSE globale mises en place par leur employeur, qui manifesteraient d'autres souhaits ou changeraient de comportements ? Nous savons déjà qu'il n'y aura pas de réponse parfaite et unique.

Quelques mots en commun pour conclure

Nous sommes convaincus que les start-up qui se créent aujourd'hui, quels que soient leurs secteurs d'activité, peuvent et doivent tout de suite intégrer les enjeux RSE dans le développement de leurs affaires, dans l'accompagnement de leurs collaborateurs et dans les interactions avec l'ensemble de leurs parties prenantes. Nous croyons que les grands groupes peuvent s'inspirer des start-up pour réviser leur modèle, y compris dans ces domaines. Enfin, nous sommes convaincus que le leader de demain est un leader responsable, qui pense le monde à long terme et agit en considérant les générations futures, sans occulter le succès économique de son organisation. ×

© Tikø


Ctrl
Alt