La data au cœur de l'enquête

Les données explosent et sont devenues les pépites du 21e siècle. Cette nouvelle dimension bouleverse le travail des forces de l'ordre et des services d'enquêtes. Avec son livre blanc, La Data au cœur de l'enquête, Deveryware aborde toutes les questions autour de cette évolution majeure et interroge des personnalités du monde de la sécurité, des nouvelles technologies et de la sphère juridique pour répondre à ces enjeux plus que jamais d'actualité. Florilège.

La data est devenue l'or noir du 21e siècle… Bien que tous ne s'accordent pas sur ce rapprochement, tant les gisements de données sont croissants et sans fin contrairement au pétrole, la nouvelle dimension portée par l'explosion du numérique et des objets connectés dont le nombre devrait avoisiner les 1000 milliards à l'horizon 2025 selon McKinsey Global Institute, fait en revanche consensus.

« Le sujet est passionnant mais complexe et ses enjeux considérables car les évolutions concernant la donnée préfigurent ce que sera l'enquête de demain, insiste Jacques Salognon, président, fondateur de Deveryware. Il méritait d'être abordé sous ses nombreux aspects : technologiques, légaux, culturels et politiques, sans oublier la dimension internationale et prospective. »

Le témoignage et les analyses de nombreux spécialistes permettent de dresser un état des lieux complet et d'établir plusieurs constats.

Complexe, fragile, polymorphe

La donnée devient essentielle pour l'investigation numérique mais les défis sont nombreux pour favoriser sa sauvegarde, éviter son altération, sa falsification.

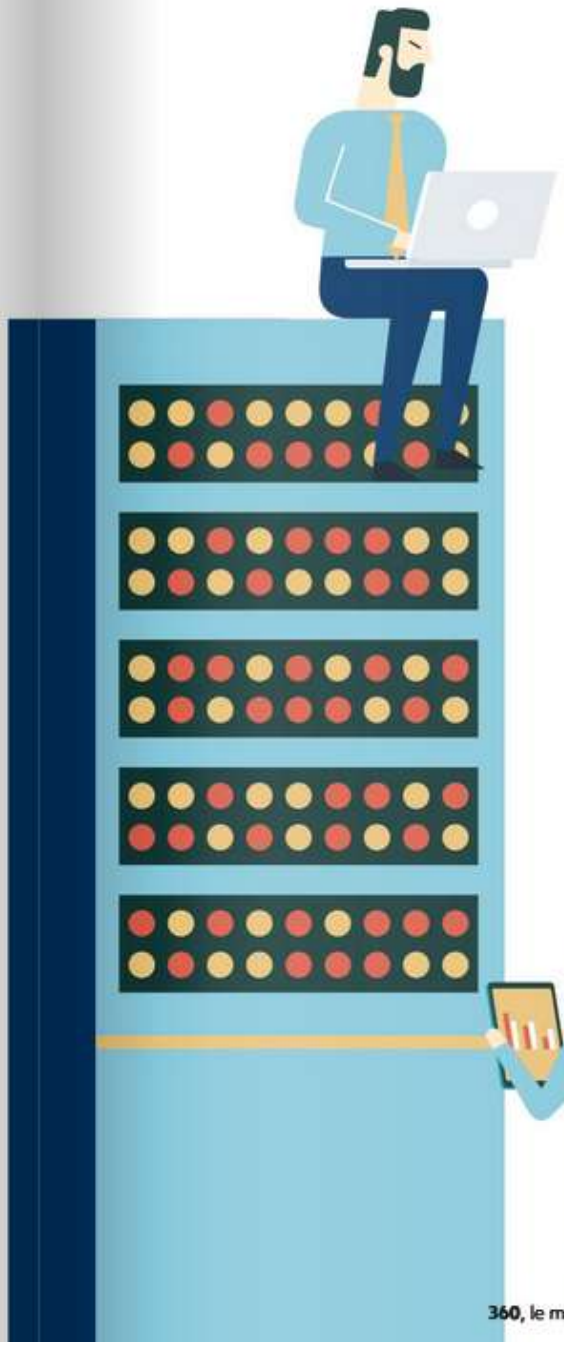
Le numérique offre un volume de données qui représente autant un atout qu'un défi. Ces données stockées représentent un coût en termes d'espace et d'énergie. Il faut savoir la capter, la ranger et la conserver au juste besoin, en conformité avec un cadre juridique évolutif et flou.

« A cette complexité, s'ajoute la problématique de la variété des données à traiter : données structurées, non structurées, données brutes ; multiplicité des formats, texte, audio, vidéo ; formats de données publiques ou privées ; lien entre les données ; textes multilingues, etc. » Thierry Bathias, directeur technique et cofondateur de Deveryware

Enfin, le Big data ne sert à rien sans la vélocité. Il faut pouvoir accéder à la donnée ou au résultat recherché rapidement.

Le retour des pirates et… des corsaires

Les technologies d'investigation doivent s'adapter car la menace investit de plus en plus le numérique (faille de réseau, fuite de données, menaces



Le volume de données numériques générées par an sera multiplié par 3,7 entre 2020 et 2025, puis par 3,5 tous les cinq ans jusqu'en 2035 (étude IDC).

ground Markets), financé par l'UE « a pour ambition de fournir aux forces de l'ordre les études dont ils ont besoin pour mettre au point de nouvelles techniques d'identification des criminels, même lorsqu'ils agissent sous couvert du pseudo-anonymat qu'offrent les monnaies virtuelles », déclare Ross King, coordinateur du projet et informaticien au Centre pour la sécurité et la sûreté numériques de l'Institut Autrichien de Technologie (AIT). « En veillant à ce que ces outils comprennent des garde-fous appropriés, nous pourrons trouver un compromis équilibré entre les besoins de confidentialité et de protection. »

De nouvelles pistes pour lutter contre les menaces

Les plateformes d'analyse offrent des

réponses adaptées à ces enjeux : traitement et exploitation de gros volumes de données et de flux d'informations en quasi-temps réel. Ces outils d'analyse représentent un potentiel encore inexploité pour lutter contre les menaces : gain de temps pour les enquêteurs, exploration de nouvelles pistes, aide à la décision, décloisonnement et partage de l'information.

Coopération et éthique

Un renforcement de la coopération entre acteurs étatiques et industriels, européens et internationaux est souhaitable. Ils doivent pouvoir évoluer dans des cadres techniques, réglementaires, éthiques et financiers transparents et cohérents. La France est confrontée à un enjeu de souveraineté technologique. Encourager une coopération public-privé et s'appuyer sur une vision stratégique commune constituent des solutions pour répondre à cet enjeu.
Les outils doivent être au service de l'intérêt général avec la nécessité de développer des plateformes intelligentes et collaboratives respectant les règlementations en vigueur en France et en Europe et s'insérant dans une approche éthique et responsable.

Nouveau monde, nouvelles menaces

Menaces multidimensionnelles, contexte stratégique instable et imprévisible, monde de plus en plus complexe et interconnecté : voici l'univers dans lequel les forces de sécurité

Une coopération public-privé renforcée : un continuum de sécurité essentiel

« A un moment où la France est confrontée à des menaces de toute nature et alors même qu'il devient nécessaire de procéder à des économies budgétaires, un changement de paradigme pourrait permettre à des entreprises privées d'intervenir dans les tâches de soutien aux forces de sécurité qui pourraient ainsi se consacrer à l'essentiel de leurs missions.
Il conviendrait d'élargir le périmètre d'action des experts techniques au profit des enquêteurs de la police, de la gendarmerie, des douanes judiciaires et des magistrats en matière de procédure pénale. » Georges Fenech, ancien magistrat et député honoraire, membre du comité stratégique de Deveryware.

œuvrent pour assurer la sécurité mondiale.

La menace terroriste est durable et investit aujourd'hui massivement le champ du numérique et des réseaux sociaux. La criminalité financière reste un phénomène complexe, croissant et coûteux et la pandémie de COVID-19 et ses retombées économiques prévues devraient probablement exacerber cette menace et créer de nouvelles vulnérabilités. La contrefaçon est un phénomène mondial qui inquiète et les menaces liées au numérique oscillent entre sophistication croissante et opportunisme. La lutte contre la criminalité, les trafics, les escroqueries ou le terrorisme se déroule aujourd'hui de plus en plus dans le cyberespace. Et les menaces y sont bien réelles.

La cybercriminalité élargit son spectre d'action année après année. Corollaire à l'apparition de nouvelles technologies (Cloud, IA, IoT, 5G…) et aux nouveaux usages, la surface d'attaque augmente continuellement. Rançongiciel, spear-phishing, cryptojacking, skimming, et sextorsion sont désormais le quotidien des enquêteurs.

Les coûts des dommages liés à la cybercriminalité sont estimés à près de 6000 milliards $ par an.

Le livre blanc La data au cœur de l'enquête est librement téléchargeable sur le site deveryware.com

La data au cœur de l'enquête

réunit parmi ses principaux contributeurs : Marc Watin-Augouard, fondateur du FIC (Forum International de la Cybersécurité), Myriam Quéméner, avocate générale à la cour d'appel de Paris et spécialiste de cybercriminalité, la lieutenante-colonelle Fabienne Lopez, cheffe du Centre de lutte contre les criminalités numériques (C3N), Alain Juillet, Président de l'Association de lutte contre le commerce illicite (ALCCI), Éric Vernier, maître de conférences à l'ISCID-CO et spécialiste du blanchiment de capitaux et des paradis fiscaux, Jean-Paul Laborde, ancien directeur exécutif du Comité de lutte contre le terrorisme du Conseil de Sécurité (CTED) des Nations Unies et l'équipe dirigeante du groupe Deveryware dont Jacques Salognon, Président fondateur et Alain Vernadat, Directeur Général.