Techniques de calcul renforçant la vie privée : un enjeu dans l'ère de la société de surveillance

Nicolas Anciaux, Benjamin Nguyen

Techniques de calcul renforçant la vie privée : un enjeu dans l'ère de la société de surveillance

Nicolas Anciaux et Benjamin Nguyen

Dans le contexte actuel du capitalisme de surveillance, tel que défini par Shoshana Zuboff dans son livre *L'Âge du Capitalisme de Surveillance*, les données personnelles sont devenues une ressource hautement convoitée par les grandes entreprises et les entités institutionnelles. Simultanément, l'intérêt croissant pour l'intelligence artificielle (IA), dont l'efficacité dépend en grande partie du volume de données disponibles, accroît colossalement le volume de collecte de données personnelles. Cette sur-collecte qui en résulte soulève des inquiétudes en matière de respect de la vie privée.

Pour répondre à cela, les autorités de régulation européennes ont instauré un cadre juridique au cœur duquel réside le Règlement Général sur la Protection des Données (RGPD), qui définit des concepts clés à respecter lors des traitements sur données personnelles, comme la présence explicite d'une finalité légitime pour le traitement, le consentement éclairé (qui doit nécessairement être obtenu auprès de l'individu concerné pour la finalité visée), la minimisation des données (une quantité minimale de données personnelles vis-à-vis de la finalité visée doit être collectée) ou encore la portabilité des données (les individus peuvent récupérer les données personnelles collectées les concernant). Bien que ces concepts semblent simples, leur mise en œuvre pratique lors du calcul, au-delà de simples injonctions juridiques est complexe pour les développeurs de solutions techniques, et constitue un frein majeur à leur adoption concrète (figure 1).

Nouveau dilemme entre surveillance et respect de la vie privée

La surveillance (et la collecte correspondante de données personnelles) vise à répondre à des objectifs légitimes, mais constitue en même temps un risque potentiel pour d'autres finalités, qui seraient elles inacceptables. Par exemple, les éditeurs de jeux en ligne (Fortnite, League of Legends, PUBG…) tracent les actions des joueurs puis exposent *via* des interfaces de programmation (API) leurs pseudonymes et leurs performances (figure 2). D'un côté, cela encourage le développement d'applications novatrices liées au jeu et l'animation de communautés de joueurs ; de l'autre, cette exposition peut permettre l'inférence d'informations sensibles (comme les pseudos d'enfants mineurs). De manière similaire, de nouveaux outils destinés à faciliter le télétravail permettent aux employeurs de surveiller l'activité de leurs employés à domicile pendant les heures de travail, mais ces données collectées pourraient également révéler des activités personnelles menées au domicile des employés. Autre exemple, la

surveillance numérique exercée par les parents sur leurs enfants à travers des logiciels de contrôle parental peut, là encore, divulguer des détails intimes sur les activités de mineurs.

Face à cette dynamique complexe, le défi consiste à concevoir de nouvelles technologies pour l'amélioration du respect de la vie privée, désignées par l'acronyme « PETs » (de l'anglais *Privacy Enhancing Technologies* ou « Technologie pour l'amélioration de la protection de la vie privée ») afin d'équilibrer les intérêts de l'ensemble des parties prenantes. Ces PETs doivent offrir aux organisations, aux individus concernés (joueurs, télétravailleurs, enfants, etc.), et développeurs d'application le moyen d'implanter les concepts du RGPD (comme la minimisation des données) afin de limiter la surveillance et contrôler les effets de bord indésirables liés à la sur-collecte. C'est une tâche ardue du fait de l'antinomie intrinsèque entre surveillance et respect de la vie privée.

Nouveaux défis scientifiques liés au calcul pour favoriser une adoption concrète de PETs

Les défis de la recherche autour des PETs résident dans la nécessité de modéliser les concepts de vie privée tout en maintenant la finalité visée. Cela requiert deux aspects clés pour une adoption concrète : premièrement, l'« explicabilité » du modèle, permettant aux développeurs de facilement implémenter le concept PET et aux individus concernés de donner leur consentement en toute connaissance de cause. Deuxièmement, il est crucial d'assurer la « confidentialité du calcul » sous-jacent (PEC, *Privacy-Enhancing Computations*) afin de permettre l'adoption du PET et d'éviter tout retour de bâton potentiel dû à un usage incorrect et des vulnérabilités qui pourraient aggraver la surveillance.

Modéliser les propriétés de vie privée souhaitées tout en assurant l'explicabilité du modèle est un problème complexe, car il implique de concilier deux dimensions conflictuelles. D'une part, pour garantir l'explicabilité, les algorithmes intégrés aux PETs doivent être publics, d'autre part, afin d'atteindre un compromis optimal entre respect de la vie privée et utilité, le comportement des PETs doit s'adapter au contenu spécifique des données personnelles de chaque individu, ouvrant ainsi la voie à d'éventuelles vulnérabilités exploitées par des attaquants. Cette complexité découle en partie de la définition ambiguë du concept de vie privée ; en particulier l'absence de définition formelle du principe de minimisation des données qui peut varier selon le contexte (données collectées à des fins d'apprentissage ou d'évaluation de règles logiques pour la prise de décision). Pour résoudre cette problématique, il est impératif de développer de nouveaux modèles qui définissent clairement ces principes dans divers contextes, fournissant ainsi aux développeurs d'applications une compréhension claire de leur implémentation. De plus, ces nouveaux modèles, une fois dotés d'une représentation intelligible, permettront aux individus de mieux appréhender les choix qui leur sont offerts et d'éclairer leur consentement.

Par ailleurs, l'intégration réussie des PETs dans le traitement de données personnelles à grande échelle nécessite non seulement de sécuriser ces données contre tout accès non autorisé, y compris de la part des créateurs et hébergeurs de PETs, mais également de relever des défis complexes liés au calcul. Les PETs opèrent sur d'énormes volumes de données, concernant potentiellement des millions d'individus, et impliquent des traitement complexes, comme la minimisation et l'anonymisation des données, intensifiant ainsi les enjeux de vie privée et de performance. L'implémentation concrète des PETs nécessite donc des solutions de calcul permettant de concilier ce double objectif de sécurité et de performance.

De nombreuses propositions de l'état de l'art portent sur la protection des systèmes de gestion de bases de données (SGBD) protégés par du chiffrement, désormais couramment fourni par la plupart des SGBD commerciaux, tels qu'Oracle et SQL Server. La gestion des clés cryptographiques est essentielle pour sécuriser les données, utilisant souvent une table restreinte ou un fichier chiffré par une clé maîtresse. Il est possible de coupler des modules de sécurité matérielle au SGBD (dits « HSM » ou *Hardware Security Module*), ce qui offre une manière de protéger les clés « au repos ». Lorsque l'application n'est pas en train de calculer, les serveurs sont protégés contre le vol ou l'exfiltration de données. Toutefois, lors du calcul, les clés et les données restent exposées (en clair) dans la mémoire du SGBD, et sont donc vulnérables aux logiciels malveillants capables d'observer la mémoire des serveurs en cours de fonctionnement.

Aller au-delà en termes de sécurité induit des solutions telles que le chiffrement homomorphe (cf. GOUBIN) permettant d'évaluer n'importe quel traitement directement sur les données chiffrées. Des protocoles de « calcul multipartite sécurisé », reposant sur ce type de technologie, sont applicables aussi en distribué, pour traiter des données confidentielles provenant de nombreux participants. Bien qu'offrant une solution théorique au problème du traitement sécurisé de données, les propositions actuelles occasionnent des surcoûts de performance très importants, liées à la complexité des traitements à réaliser et au nombre élevé des participants au calcul, ce qui les rend le plus souvent impraticables dans le contexte des PETs. En effet, la solution MPC (calcul multipartite sécurisé) la plus connue est basée sur l'utilisation de « *garbled circuits* », qui permettent de transformer un algorithme en circuit logique. Ce circuit peut ensuite être évalué de manière sécurisée, en présence d'adversaires « honnêtes-mais-curieux ». Chaque participant apporte au calcul ses données privées, sans les révéler à l'autre. Il est toujours possible de généraliser à un nombre plus grand de N participants, mais le coût en nombre de communications entre les participants croît quadratiquement avec leur nombre (théorème BMR, de Beaver, Micali, Rogaway). Des résultats plus récents évaluent le coût à deux messages par porte 'ET' dans le circuit. Les performances du calcul dépendent ainsi également de la complexité du code de l'algorithme. Dans cette approche, l'algorithme à évaluer est connu de l'ensemble des participants (ce qui est aussi une limite).

Pour surmonter les défis liés à la performance du traitement sécurisé, la dernière décennie a vu l'avènement de nouveaux composants de l'informatique, comme les processeurs dotés d'environnements d'exécution de confiance matériels (par exemple, *Intel SGX Software Guard Extensions*, *ADM SEV Secure Encrypted Virtualization*, *ARM Trustzone*, *Intel TDX Trust Domain Extensions*). Ces environnements créent un espace de traitement des données (enclave) résistant à la manipulation. Il repose sur deux mécanismes fondamentaux : l'isolation, qui préserve la confidentialité des données traitées dans l'enclave vis-à-vis du système d'exploitation ; et l'attestation, qui permet au code du traitement de fournir une preuve cryptographique de son identité, certifiant qu'il fonctionne au sein d'une enclave authentique. Ce double mécanisme garantit à la fois la confidentialité des données en cours d'utilisation et l'intégrité du traitement. Comme pour toute solution de sécurité « matérielle », cette technologie présente certaines limitations techniques, en termes de gestion de la mémoire, de performance et de surcoût lié aux échanges de données entre l'enclave et l'extérieur. Par exemple, en 2015, la première version d'Intel SGX offrait une taille de mémoire limitée à 128 MB. Cette mémoire est utilisée pour stocker le code, les données et la pile d'exécution de l'enclave. Ainsi, si une application nécessite plus de mémoire que ce qui est disponible, elle doit utiliser des mécanismes de pagination, où les données sont échangées entre l'enclave et la mémoire externe non protégée. Cela peut entraîner des ralentissements significatifs en raison des opérations de chiffrement/déchiffrement et de la vérification de l'intégrité des données échangées. Les applications peuvent également être conçues pour minimiser la nécessité de communication entre l'enclave et la partie non sûre, réduisant ainsi les effets négatifs sur la performance. D'autres part, la sécurité matérielle conduit à d'autres types de contraintes pour pallier certaines attaques. Deux types d'attaques existent sur du matériel sécurisé : celles qui nécessitent une contre-mesure du fabricant (la prochaine version du dispositif intègrera alors cette contre mesure) et celles qui nécessitent une réponse au niveau du développeur d'application (le code de calcul qui tourne sur le matériel sécurisé doit alors être modifié pour prendre en compte une nouvelle contrainte et éviter l'attaque). La contre mesure consiste à intégrer des techniques logicielles au sein du code du calcul visant à masquer les motifs d'accès aux données. Ainsi, bien qu'offrant une solution générique plus performante que les solutions cryptographiques comme le MPC, les solutions matérielles ont des contraintes spécifiques à différents niveaux qui influent sur la performance du calcul et la complexité des développements. Permettre aux SGBD d'exploiter ces propriétés de sécurité matérielle et donc prévenir la manipulation en clair de données sensibles à l'extérieur de l'enclave reste encore un défi.

Conclusion

Surveillance, préservation de la vie privée et sécurité des personnes requièrent une convergence harmonieuse entre les avancées de la cybersécurité et les besoins d'innovation technologique en

termes de PETs utilisables pour les utilisateurs et permettant d'assurer les principes légaux inscrits dans la règlementation européenne (RGPD). Nous travaillons à la création de processus permettant de faire émerger une nouvelle génération de PETs respectant ces objectifs, intégrant à la fois des techniques d'évaluation explicables et des solutions de calcul sécurisé efficaces sur de grands volumes de données.

Figures

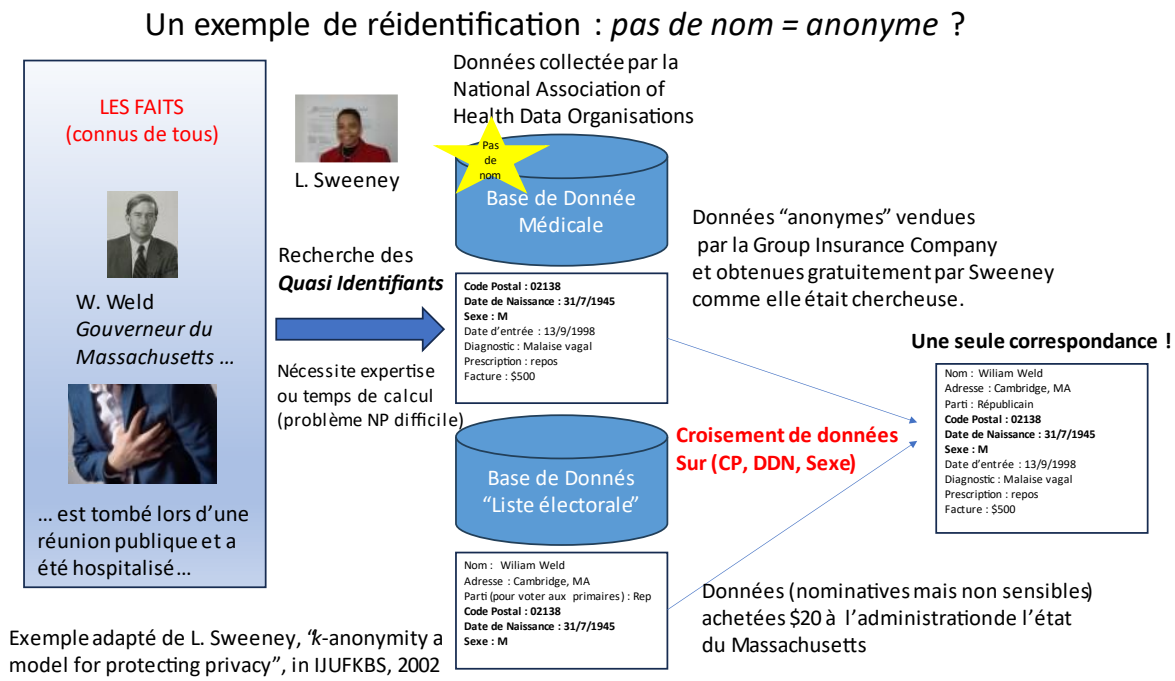

Figure 1. L'attaque de réidentification de Sweeney

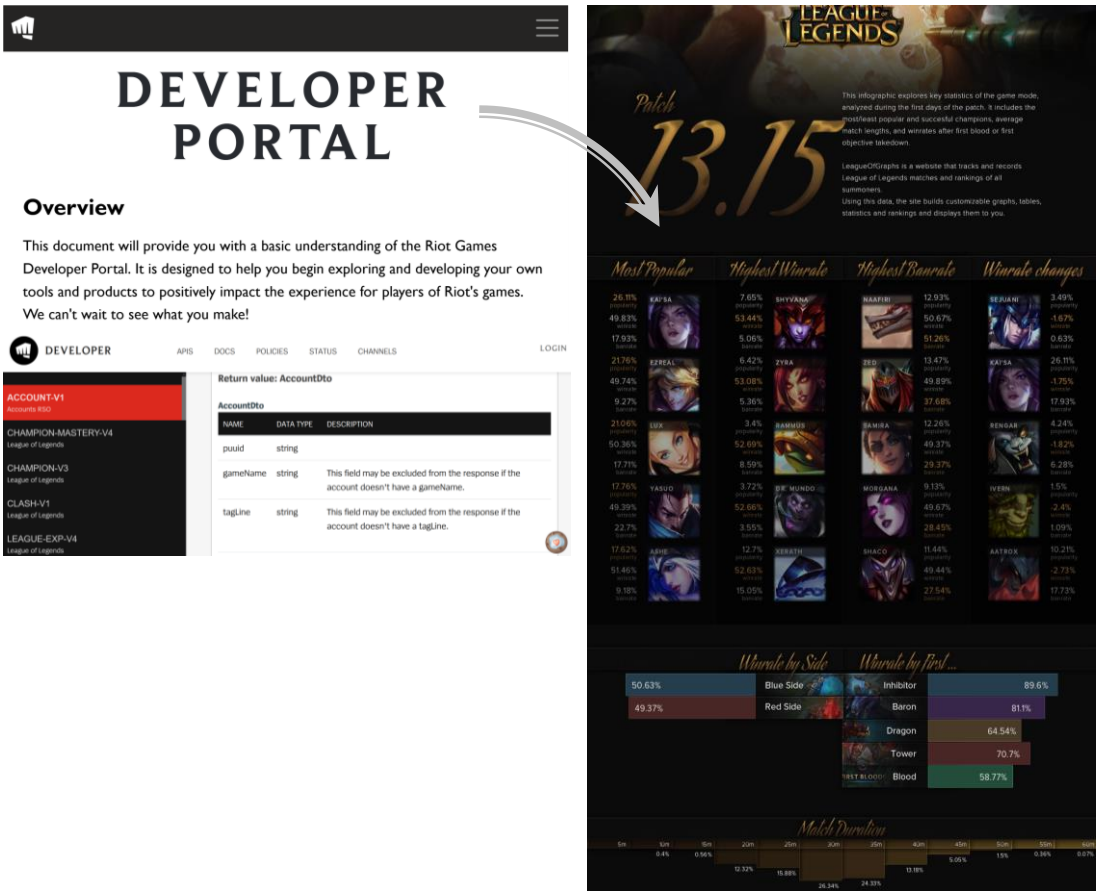

Figure 2. Site de la société américaine « Riot Games » qui édite le jeu vidéo *League of Legends* dédié aux développeurs, qui indique comment accéder à certaines données des joueurs, et leur permet de produire des synthèses et statistiques par exemple lors de l'organisation de tournois en ligne.

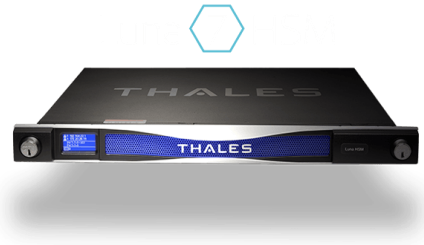

Figure 3. Le HSM Luna de la société française Thalès

Bibliographie

Shoshana Zuboff, *The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power,* Public Affairs, New York, 2019. Article librement accessible de l'auteure sur le même sujet dans le monde diplomatique : https://www.monde-diplomatique.fr/2019/01/ZUBOFF/59443

Journal Officiel de la Commission Européenne, Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Texte intégral : https://eur-

lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679. Présentation de la CNIL : https://www.cnil.fr/fr/reglement-europeen-protection-donnees

Christian Paul et Daniel Le Métayer, *Maîtriser l'IA au service de l'action publique* : *une responsabilité individuelle et collective*, Berger Levrault, Au fil du débat, 2023.

Tangente Hors-série n°52. Mathématiques & Informatique. *Limiter la collecte des données personnelles : Un problème juridique NP-difficile*, par Nicolas Anciaux et Benjamin Nguyen, pp. 76-80, Juin 2014. Version de l'article accessible en ligne : https://www.benjamin-nguyen.fr/papers/tangente2014.pdf

Nicolas Anciaux, Luc Bouganim et Yanli Guo (2023). Database Encryption. In: Jajodia, S., Samarati, P., Yung, M. (eds) Encyclopedia of Cryptography, Security and Privacy. Springer, Berlin, Heidelberg. Accessible en ligne : https://link.springer.com/referenceworkentry/10.1007/978-3-642-27739-9_677-2 (Lien HAL : https://hal.science/hal-04346550)

Affiliation

Nicolas Anciaux. Gestion de données personnelles, sécurité et vie privée, Directeur de Recherche Inria, Inria de Saclay, laboratoire DAVID, Université Paris-Saclay – Versailles, Nicolas.Anciaux@inria.fr

Benjamin Nguyen. Gestion de données personnelles, sécurité et vie privée, Professeur des Universités, Laboratoire d'Informatique Fondamentale d'Orléans, INSA Centre Val de Loire et Université d'Orléans, benjamin.nguyen@insa-cvl.fr

Glossaire

API (*Application Programming Interface*). Ensemble de fonctions proposées par une application (par exemple via un serveur Internet) qui peuvent, entre autres, permettre de récupérer des données.

Calcul Multipartite Sécurisé (SMC ou MPC). Algorithmes distribués permettant de réaliser des opérations avec des garanties formelles de sécurité et de confidentialité.

Chiffrement homomorphe (appelé aussi FHE). Technique de chiffrement qui permet à un serveur d'exécuter des opérations mathématiques (comme des additions ou des multiplications) sans avoir besoin de déchiffrer des données, tout en produisant un résultat correct pour la personne capable de déchiffrer les données.

Hardware Security Module (HSM). Serveur dont le rôle est uniquement de stocker des clés de chiffrement. L'intérêt est que pour pouvoir déchiffrer les données un attaquant doit d'une part se procurer les données sur le serveur d'application et d'autre part réussir à se procurer la clé en s'introduisant dans le HSM. La difficulté de réaliser une attaque est ainsi « doublée ».

Théorème BMR. Ce théorème énonce qu'il existe un protocole cryptographique à N participants, pour lesquels une majorité est honnête, permettant de calculer tout circuit de manière sécurisée. Le

protocole utilise un nombre constant de rounds et un nombre de communications polynomial dans le nombre de participants.

Pagination. La pagination est une technique informatique permettant de gérer l'accès à la mémoire de manière organisée et efficace. La mémoire virtuelle est divisée en "pages" de taille fixe (par exemple 4KB par page) et un algorithme fait correspondre chaque page à un emplacement de mémoire physique via une table de pagination. Dans le cas spécifique d'Intel SGX (Software Guard Extensions), la mémoire virtuelle de l'enclave est divisée en pages sécurisées, chiffrées et attestées pour garantir leur intégrité et confidentialité. La table de pagination est appelée EPC (Enclave Page Cache). Lorsqu'un programme s'exécute à l'intérieur d'une enclave SGX, l'accès à la mémoire est géré par ce mécanisme de pagination, assurant que les données sensibles restent isolées et protégées contre les accès non autorisés, y compris par le système d'exploitation et d'autres applications.