

Facteur humain, la ludification au service de la sensibilisation



Adrien CHAMBADE

Président

ONYL Rocks | CyberLudik

La sensibilisation, cette pratique qui s'attache à faire changer les comportements des personnes qui en font l'objet, se démocratise depuis plusieurs années. On la retrouve par exemple dans des contextes de prévention, au sein d'exigences normatives, par exemple avec ISO 27001¹, et même légales, par exemple avec le RGPD l'introduisant via les missions du délégué à la protection des données². Il convient alors de déterminer les objectifs que l'on se fixe lorsqu'on organise une campagne de sensibilisation, puis de choisir la façon avec laquelle l'appréhender, sa temporalité et les moyens à mettre en œuvre. Dernièrement, des initiatives plus ou moins industrialisées ont fleuri en profitant de l'essor du « serious game », des jeux sérieux adoptant une approche ludique qui tente de remobiliser les collaborateurs fatigués des

présentations magistrales, des recueils de bonnes pratiques servant à caler un meuble ou des webinaires qui remplacent la musique de fond. La présente tribune ne vient pas jeter la pierre à ces approches, mais va tenter d'apporter un éclairage sur le recours à des mécaniques davantage ludiques, plus complexes à mettre en œuvre mais complémentaires des pratiques traditionnelles.

Le jeu, un réel intérêt ?

Le recours à la pratique du jeu dans nos organisations pour réaliser les campagnes de sensibilisation n'est pas uniquement un argument marketing, mais s'avère être un levier à bien des égards. L'impact du jeu synthétisé par L. Sauvé, L. Renaud et M. Gauvin³ dans cette transmission s'avère pertinent car :

- il constitue un levier permettant de motiver les participants et de renforcer la confiance en soi, notamment grâce à l'aspect compétitif ;
- il favorise la coopération, notamment face à la nécessité d'échanger devant un groupe, de négocier ou de travailler en équipe ;
- il développe la logique et améliore l'esprit des joueurs à résoudre un problème, à prendre des décisions ou à arbitrer un choix ;
- il permet l'intégration des concepts et des informations par un moyen détourné, structurant notamment les connaissances de chacun.

L'approche par le jeu, a fortiori lorsqu'il s'agit d'une action « en présentiel » autour d'un plateau, aussi

¹ ISO/IEC 27001:2022(F), Clause 7.3 et Exigence 6.3 de l'annexe A (Tableau A.1 — Mesures de sécurité de l'information)

² Règlement (UE) 2016/679 du Parlement européen, Article 39 - Missions du délégué à la protection des données

³ Une analyse des écrits sur les impacts du jeu sur l'apprentissage, Université du Québec à Montréal, un article de la Revue des sciences de l'éducation (Volume 33, numéro 1, 2007, p. 89–107), <https://www.erudit.org/fr/revues/rse/2007-v33-n1-rse1732/016190ar/>

magnifique soit-il, se doit néanmoins de prendre en considération l'animateur : ses aptitudes, connaissances et compétences en la matière ; il se devra en effet, comme le rappellent E. Tremblay-Wragg, C. Raby et L. Ménard reprenant la recherche d'Halawah (2011)⁴ d'être enthousiaste, ouvert, disponible et attentif au déroulé du jeu pour, par exemple, créer des échanges individualisés et nouer une relation affective, ou de confiance tout du moins. Cette posture aura comme avantage premier de favoriser naturellement l'implication des participants et de créer un espace d'échanges sérieux mais également décontractés.

Quel impact du jeu dans un contexte de cybersécurité et de protection des données personnelles ?

S'appuyant sur leurs connaissances et leur capacité à communiquer, la tâche de sensibiliser incombera généralement aux RSSI (Responsable de la Sécurité des Systèmes d'information)⁵ ou aux DPO (Délégué à la Protection des Données, DPD en français)⁶. A défaut, elle pourra être réalisée par des intervenants extérieurs qui devront alors connaître à la fois le sujet et le contexte de l'organisme dans lequel se déroule l'activité. Le jeu ne peut se substituer à l'ensemble des actions mises en œuvre pour sensibiliser les collaborateurs, mais crée une occasion fédératrice, permettant d'ancrer le sujet à travers un support palpable, dans un contexte indépendant de l'activité quotidienne, favorisant ainsi la concentration, l'implication et l'immersion des collaborateurs.

⁴ En quoi la diversité des stratégies pédagogiques participe-t-elle à la motivation à apprendre des étudiants ? Etude d'un cas particulier, Émilie Tremblay-Wragg, Carole Raby et Louise Ménard, <https://journals.openedition.org/ripes/1288>

⁵ Enquête auprès des responsables de la sécurité des systèmes d'information (RSSI), ANSSI, 2021, <https://www.ssi.gouv.fr/uploads/2021/10/anssi-profil-de-la-cybersecurite-enquete-rssi.pdf>

⁶ Guide pratique RGPD - Délégués à la protection des données, CNIL, 2022, https://www.cnil.fr/sites/default/files/atoms/files/guide_prat

Si l'on souhaite en maximiser son impact, l'activité de sensibilisation doit également viser à élever le niveau des participants en évitant si possible de démarrer de zéro, cette situation initiale contournant ainsi l'accueil nécessitant alors de varier les supports et les stratégies, ce qui peut rapidement s'avérer contraignant, comme l'ont repéré Joyce et al., 2015⁷. Sur ce point, l'expérimentation menée en février 2023 auprès des étudiants de licence professionnelle ESSIR de l'IUT Lyon 1 a pu montrer, grâce à un jeu de société sur le RGPD⁸ joué après avoir formés les apprenants, une amélioration médiane de 10% de l'appropriation des concepts de protection des données personnelles et des comportements conformes afin d'assurer cybersécurité et respect de la vie privée des personnes concernées.

Un format intéressant peut par exemple se décliner en trois temps : la présentation dans un premier temps du concept et des définitions fondamentales, puis la phase de jeu reprenant comme règles les éléments présentés précédemment, et enfin la phase d'échanges et de remédiation donnant la parole aux participants pour poser leurs questions et à l'animateur pour conclure - ce dernier temps peut s'avérer pertinent pour traiter de spécificités liées à l'organisme ou relater des faits d'actualité.

Une indéniable nécessité d'innover dans nos approches pédagogiques ?

Le chiffre varie selon les études mais, d'après une étude d'IBM⁹, l'erreur humaine peut être rencontrée dans plus de 95% des incidents de sécurité. Force est de constater que l'humain est - et restera encore

[igue rgpd - delegues a la protection des donnees.pdf](#)

⁷ En quoi la diversité des stratégies pédagogiques participe-t-elle à la motivation à apprendre des étudiants ? Etude d'un cas particulier, Émilie Tremblay-Wragg, Carole Raby et Louise Ménard, <https://journals.openedition.org/ripes/1288>

⁸ Jeu plateau CyberLudik RGPD & Sécurité, <https://cyberludik.fr/store/jeu-de-societe/pro/cyberludik-rgpd-secureite/>

⁹ IBM Security Services 2014 Cyber Security Intelligence Index, <https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF>

longtemps - le maillon le plus faible dans l'empilement des lignes de défense mises en place pour protéger nos systèmes d'information.

Que l'on œuvre au sein d'associations, de collectivités territoriales, de TPE, PME ou de grands groupes, le point commun reste l'humain. Malgré des cultures potentiellement différentes selon la typologie ou le secteur de l'organisme, les comportements iront nécessairement vers la productivité au détriment de la conformité, et par extension, de la sécurité. Faire changer les comportements ou prévenir tout écart revêt une importance indiscutable. Néanmoins l'approche se doit d'être travaillée, la mécanique adaptée au sujet, et le calibrage défini pour récompenser les comportements que l'on souhaite faire adopter. Pour satisfaire cela, il ne faut pas hésiter à étudier longuement son environnement, à construire son jeu de façon itérative, et éventuellement à s'appuyer sur les outils pertinents du secteur, qu'il s'agisse de jeux existants ou d'outils de création assistée. Chacun pourra donc s'emparer du sujet au sein de son organisme et pourra, comme le confirme l'étude de Jane McGonigal¹⁰ qui précise les points essentiels à considérer dans la conception ou le choix d'un jeu, s'assurer que le jeu intègre des objectifs clairs, des situations variées, une immersion forte, des conséquences concrètes et une façon simple permettant aux joueurs d'évaluer leur performance.

La sensibilisation par le jeu dans le contexte de la cybersécurité, notamment grâce à des jeux de plateau, tangibles, aura donc une utilité bien réelle qui pourra à la fois assurer conformité et sécurité dans l'organisme, et proposer une approche décalée devenant nécessaire aujourd'hui pour continuer à tenir le discours dans notre domaine d'activité.

Et vous ? Quelle approche adoptez-vous ?

¹⁰ Jane McGonigal, Reality is Broken. Why Games make us Better and How They can change the World, 2011