



DOSSIER

Transitions et sécurité numériques

Réalisé par Christophe Bonnet, Florence Dubonnet et Laurent Kaufmann.

Les transitions numériques comptent parmi les plus importantes transformations à l'œuvre au XXI^e siècle. Si elles prennent des formes diverses, toutes interrogent notre rapport au monde et à la société que nous voulons construire.

Elles interrogent, par exemple, l'inclusion – car il y a aussi des exclu-e-s du numérique –, nos manières de travailler, nos relations au collectif, l'écologie...

Ce dossier aborde plus particulièrement la question de la sécurité et de l'insécurité dans ces transitions auxquelles nous faisons face au travail et dans la gouvernance de nos ministères. Un sujet, aussi, profondément syndical !

Universités et sécurité informatique



© Kalih / Pixabay

Les récentes cyberattaques subies par des universités¹ ont eu des conséquences majeures sur le service rendu et sur le travail des agents. Pourtant, la sphère de l'enseignement supérieur et de la recherche était plutôt mieux préparée que les autres services publics à la transition numérique : c'est par elle qu'Internet était arrivé en France, dès la fin des années 1980, avant de se diffuser dans le grand public. Les services informatiques des universités avaient un solide bagage professionnel, issu de leurs contacts avec le monde de la recherche; et leurs ingénieurs avaient conservé une solide culture du « faire » plutôt que de dépendre exclusivement de compétences externes.

Force est de le constater : cet avantage initial s'est largement érodé au cours des vingt dernières années. D'abord, parce que, comme pour toutes les fonctions support, les moyens disponibles n'ont pas progressé au même rythme que les besoins. Ensuite, parce que le défaut d'attractivité de ces métiers s'est largement aggravé : stagnation des rémunérations indiciaires, indemnitaire insuffisant et illisible². Les recrutements de contractuels se sont multipliés, augmentant d'autant la vitesse de rotation des agents sur les postes.

Les directions des systèmes d'information se trouvent donc aujourd'hui bien en deçà des effectifs minimum qui leur seraient nécessaires, alors que la charge de travail augmente, et que le caractère indispensable des ressources numériques les soumet toujours plus à une obligation permanente de résultat. C'est à ce déséquilibre qu'il convient en urgence de répondre si l'on veut prévenir de futures attaques contre les systèmes d'information des universités. • C. B.

¹Paris-Saclay en aout et Paris I – Panthéon-Sorbonne en octobre derniers. Cf. « Sécurité des SI, saison 2. La cybersécurité au cœur de la stratégie de l'ESRI », *La collection numérique*, # 31 – février 2024, Amue, <https://urlz.fr/t5PO>

²<https://urlz.fr/t5Pm>

LA GRANDE PROMESSE DU NUMÉRIQUE EST LE PROGRÈS. Si certains de ses apports sont indéniables, il comporte aussi de nombreux écueils...

INSÉCURISATION(S)

L'arrivée de nouveaux outils peut, certes, se faire naturellement (le livret scolaire du lycée a avantageusement remplacé les dossiers papier), mais dans de trop nombreux cas, des transitions du travail par le numérique, mal pensées et mal accompagnées, insécurisent les agents. « J'avais l'impression de ne plus rien connaître de mon métier, moi qui me sais expert dans mon domaine », témoigne un fondé de pouvoir confronté au passage à Op@le, le nouvel outil de gestion comptable et financière des établissements publics locaux d'enseignement (EPL). Une application dont les objectifs sont, selon le ministère, de faciliter le travail des utilisateurs, d'améliorer la sécurité des processus et du cadre technique, et de renforcer la qualité « métier » (sécurisation des échanges de données entre applications, meilleure traçabilité des opérations...). Or, confiée essentiellement à des sociétés externes, la conception d'Op@le, avec ses nombreux bugs

malgré un développement sur le temps long et un déploiement pensé en phases successives, a mis à mal plusieurs milliers de personnels. De même, la mise en place de l'application RenoiRH pour la gestion des personnels ingénieurs, administratifs, techniques, sociaux et de santé, faute d'avoir anticipé les changements qu'elle allait entraîner dans la manière de travailler, a rudement éprouvé les services RH des rectorats. Ce qui est également insécurisé, c'est le service rendu (par exemple avec RenoiRH, décalage de la paie pour des contractuels). Finalement, l'outil de travail empêche parfois le travail ! La liste malheureusement s'allonge car, avec des nuances, on pourrait citer Lien, le logiciel infirmier de l'Éducation nationale; Esculape, celui des médecins scolaires; OSE en université, ou encore Siham.

LÀ OÙ LE BÂT BLESSE

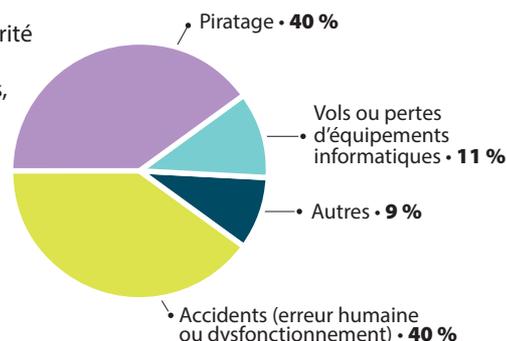
Ce qui est en cause est à analyser au plus près de la réalité : comment se fait le développement d'une application et quelle place est donnée aux utilisateurs lors de sa conception ? Quel accompagnement des équipes ? Quelles formations adaptées – tout changement étant du travail en plus ?

Origines des violations de données dans les établissements de l'Enseignement supérieur et de la Recherche depuis 2018.

D'après la Cnil, les incidents de sécurité frappent les établissements de tous types et de toutes tailles, universités, grandes écoles ou organismes de recherche.

Sur les 17 500 violations de données qui lui ont été notifiées depuis 2018, 380 (environ 2%) concernaient directement un établissement d'ESR.

Source : *La collection numérique* #31 (cf. références ci-contre), page 26.





© Gerait / Pixabay

Les personnels des directions des systèmes d'information alertent sur les risques de cyberattaque.

Parfois, le souci est aussi qu'un logiciel a deux objectifs : servir le travail et le pilotage. Or, souvent, il ne fait bien ni l'un ni l'autre !

En tant qu'organisation syndicale, nous pouvons agir sur tous ces aspects, depuis l'équipe de travail concernée jusqu'aux niveaux académique et national.

Et, au-delà de ces applications, chacun doit s'interroger sur les outils utilisés au quotidien : ont-ils bousculé mon travail, dans quelle mesure ? M'ont-ils apporté plus de confort, de meilleurs traitements des infor-

mations, un allègement de ma charge de travail ?

QU'EN EST-IL DES DONNÉES ?

Les Gafam ont fait des données un objet de commerce à échelle mondiale. Dès lors, les enjeux en sont à la fois commerciaux et politiques. En effet, qu'il s'agisse des données propres aux agents ou de celles nécessaires à l'accomplissement de nos missions de service public, la question se pose de leur stockage, de leur usage et de leur protection.

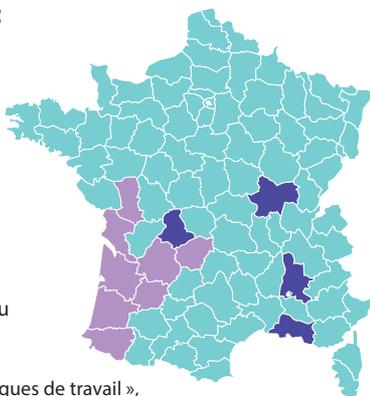
Cet été, un incident majeur de la sécurité des accès aux systèmes d'information a eu lieu à l'université Paris-Saclay (lire p. 8). Le cas n'est pas isolé. Les personnels des directions des systèmes d'information (DSI) alertent sur ces risques de cyberattaque et sur l'augmentation nécessaire des niveaux de sécurisation des accès. Nous sommes ainsi de plus en plus souvent soumis à une double authentification pour rejoindre nos univers professionnels numériques.

Nous pouvons aussi nous interroger sur la manière dont l'État s'assure de la sécurité des données qui concernent les usagers, et en premier lieu les élèves. Ainsi l'application Pronote, malgré l'entrée de Docaposte dans sa gouvernance, est-elle complètement sécurisée ? Est-il normal que l'emploi du temps, donnée centrale de la vie des EPLE, dépende quasi entièrement de la société privée Index Éducation ? Ce logiciel renforce aussi le contrôle des EPLE sur la mise en œuvre des réformes, par exemple les groupes de niveaux et de renforcement de courte durée. On est loin de l'École de la confiance.

En matière de ressources humaines, la Cour des comptes s'inquiète de l'arrivée de Virtuio, un logiciel de gestion des recrutements contractuels : « La solution d'hébergement offerte par le prestataire repose sur une entreprise états-unienne ; il ne peut dès lors être totalement exclu que des données à caractère personnel soient stockées ou transitent hors du territoire de l'Union européenne, ou encore qu'en application de la législation des États-Unis, le prestataire fasse l'objet d'une injonction de communication des données qu'il héberge de la part des autorités de cet État ». Même si un accord, permettant d'assurer un équivalent de notre RGPD, fait dire à la Cour que le ministère de ●●●

Cartographie du déploiement des espaces numériques de travail (ENT) dans les collèges publics à la rentrée scolaire 2023.

- 80 % - 100 %
Déploiement massif
- 1 % - 79 %
En cours de déploiement
- 0 %
Pas de projet ENT ou inconnu



Guadeloupe



Martinique



Réunion



Guyane



Mayotte



Saint-Pierre et Miquelon



Wallis et Futuna



Polynésie française



Nouvelle Calédonie



« L'état du déploiement des espaces numériques de travail », Eduscol : <https://urlz.fr/endD>



Laurent Kaufmann* “l’informatique est partout à l’École”

* PERSONNEL DE DIRECTION ET SECRÉTAIRE FÉDÉRAL
DE LA CFDT ÉDUCATION FORMATION RECHERCHE PUBLIQUES.



l’Éducation nationale et de la Jeunesse est « potentiellement exposé à un risque d’image », on peut se demander si le risque ne va pas au-delà.

En tant qu’organisation syndicale, nous avons notre mot à dire sur tous ces sujets de gouvernance des systèmes d’information – notamment via les comités sociaux d’administration (CSA).

UN SUJET RH

Piloter ces systèmes demande une haute technicité et de l’expertise. Or, les DSI peinent à recruter. Les niveaux de rémunération indiciaire et indemnitaire pour les titulaires n’attirent pas, surtout en début de carrière. Le recrutement de contractuels n’est pas plus simple, les salaires peinant à suivre le marché. L’appel à des sociétés externes est aussi de plus en plus répandu. Il y a donc un sujet RH, qui touche d’ailleurs tous les métiers de l’informatique.

Sur ces sujets, comme sur d’autres, la CFDT Éducation Formation Recherche Publiques continue d’interroger ce que cela produit à la fois sur le travail et sur le service public. À nous de faire que le numérique soit d’abord un outil de progrès pour toutes et tous.

¹ « La fonction ressources humaines au ministère de l’Éducation nationale », rapport public thématique de la Cour des comptes, octobre 2024, p. 100 et 101, <https://urlr.me/PEJaTw>

Quels sont les principaux risques en matière de sécurité informatique ?

● Le risque majeur dans les établissements publics locaux d’enseignement (EPLE) provient de l’utilisation de bases de données contenant des informations personnelles, parfois sensibles (données médicales). De plus, les usagers (professionnels, parents, élèves) ne sont pas également sensibilisés aux risques et sont souvent très peu formés.

Aujourd’hui, quasiment tous les collèges et lycées publics utilisent des espaces numériques de travail (cf. carte p. 9), en général interfacés avec des logiciels de gestion des notes et des absences (majoritairement Pronote). Ces outils permettent à tous les personnels de communiquer au quotidien, et aux familles de suivre la scolarité de leurs enfants. S’y ajoutent aussi les applications pour la saisie des demandes de bourse ou des vœux d’orientation. Bref, l’informatique est partout à l’École. Le premier risque réside donc dans la méconnaissance des usagers de la charte informatique que tout établissement doit faire connaître. L’accès à ces outils (qu’il s’agisse de maîtriser suffisamment l’écrit ou de disposer du matériel informatique) est un écueil important. Il désavantage les familles défavorisées.

Qui gère ces risques et comment ?

● Le premier responsable du bon usage et du respect des données est bien sûr le chef d’établissement. Ce qui peut parfois être un peu écrasant. Le risque n’est pas qu’interne : la menace d’alerte à la bombe, d’attaque terroriste (provenant aussi bien d’élèves que d’éléments extérieurs pour déstabiliser les établissements) peut être si forte qu’au moment des épreuves d’examen, il a pu être décidé de couper l’accès aux outils de messagerie. En cas de mésusage des outils ou de fuite des données, la Cnil peut être saisie et elle

peut mettre en demeure l’établissement de se conformer aux règles de droit.

Qu’en est-il de la formation ?

● Le temps étant compté dans les EPLE, il est complexe de mettre en place de la formation adaptée à la gestion des outils de communication numérique et à leurs risques. C’est cependant indispensable car le numérique est maintenant partout dans la vie des usagers, parfois pour le pire (harcèlements, conflits graves entre élèves...). La pression scolaire peut aussi être renforcée par un usage irraisonné du suivi des notes, notamment lors des paliers d’orientation.

Cette formation, qui peut être dispensée par le référent numérique en établissement, représente un temps de travail important, et avec la baisse des dotations, il devient de plus en plus délicat de trouver des personnels motivés.

Quel est ton point de vue en tant que militant ?

D’un point de vue syndical, le numérique est une bonne occasion de parler du travail des agents et des élèves. Les applications informatiques, censées améliorer le quotidien, renforcent souvent la dégradation des conditions de travail ou de l’accès au droit des usagers. L’application Op@le a désorganisé profondément la vie des établissements. D’abord des services de gestion mais aussi des usagers en retardant le paiement des bourses ou en empêchant la tenue de voyage pédagogique. Et que dire de l’accord Télétravail qui peine à se mettre en place, notamment en raison de l’absence de matériel informatique. La CFDT Éducation Formation Recherche Publiques est en pointe sur ces combats pour une amélioration des conditions de travail de tous les acteurs de la communauté éducative.