

N° 142

# SÉNAT

SESSION ORDINAIRE DE 2021-2022

---

---

Enregistré à la Présidence du Sénat le 10 novembre 2021

## RAPPORT D'INFORMATION

FAIT

*au nom de la délégation aux entreprises (1) rendant compte de la **Journée des entreprises organisée au Sénat le 21 octobre 2021,***

Par M. Serge BABARY,

Sénateur

---

(1) Cette délégation est composée de : M. Serge Babary, *président* ; M. Stéphane Artano, Mmes Martine Berthet, Florence Blatrix Contat, MM. Gilbert Bouchet, Emmanuel Capus, Mme Anne Chain-Larché, MM. Gilbert-Luc Devinaz, Thomas Dossus, Fabien Gay, Jacques Le Nay, Dominique Théophile, *vice-présidents* ; MM. Rémi Cardon, Jean Hingray, Sébastien Meurant, Vincent Segouin, *secrétaires* ; Mmes Cathy Apourceau-Poly, Annick Billon, Nicole Bonnefoy, MM. Michel Canevet, Daniel Chasseing, Alain Chatillon, Mme Marie-Christine Chauvin, M. Pierre Cuypers, Mme Jacky Deromedi, M. Alain Duffourg, Mme Pascale Gruny, MM. Christian Klinger, Daniel Laurent, Martin Lévrier, Didier Mandelli, Jean-Pierre Moga, Albéric de Montgolfier, Claude Nougéin, Mme Guylène Pantel, MM. Georges Patient, Sébastien Pla, Mmes Émilienne Poumirol, Frédérique Puissat, MM. Christian Redon-Sarrazy, Olivier Rietmann, Daniel Salmon.



## SOMMAIRE

	<u>Pages</u>
<b>AVANT-PROPOS .....</b>	<b>3</b>
<b>PROGRAMME DE LA JOURNÉE .....</b>	<b>5</b>
<b>I. OUVERTURE .....</b>	<b>13</b>
<b>II. THÈME 1 : LA CYBERSÉCURITÉ DES ENTREPRISES .....</b>	<b>19</b>
A. TABLE RONDE : « COMMENT RÉPONDRE À L'URGENCE ? » .....	19
B. DÉBAT .....	24
<b>III. THÈME 2 : PRÉVENTION EN SANTÉ ET BIEN-ÊTRE AU TRAVAIL .....</b>	<b>39</b>
A. PRÉSENTATION DES ÉVOLUTIONS INTRODUITES PAR LA LOI « SANTÉ AU TRAVAIL » .....	39
B. TABLE RONDE : « QUELS OUTILS POUR UN NOUVEAU MONDE DU TRAVAIL ? » .....	41
C. DÉBAT .....	48



## AVANT-PROPOS

La Délégation sénatoriale aux entreprises a organisé au Sénat jeudi 21 octobre 2021 la cinquième édition de la Journée des entreprises, événement organisé chaque année depuis la création de la Délégation en novembre 2014, à l'initiative du Président du Sénat, M. Gérard Larcher.

Rassemblant 42 sénateurs désignés à la proportionnelle des groupes politiques, cette Délégation est chargée d'informer le Sénat sur la situation des entreprises, de recenser les obstacles à leur développement et de proposer des mesures visant à favoriser l'esprit d'entreprise et à simplifier les normes applicables à l'activité économique, en vue d'encourager la croissance et l'emploi dans les territoires.

Depuis janvier 2015, la Délégation est allée à la rencontre de centaines d'entrepreneurs français dans plus de 30 départements, ainsi que dans quelques pays européens. Sur le fondement des témoignages de terrain ainsi recueillis, elle intervient en posant des questions au Gouvernement et en élaborant des propositions de loi, des propositions de résolution, des rapports ainsi que des amendements aux projets de loi concernant les entreprises. Elle conduit aussi des études utiles pour éclairer le vote du Sénat sur les dispositions ayant un impact sur l'entreprise. Enfin, elle contribue à une meilleure information de tous sur les défis que doivent relever les entreprises et les enjeux pour le dynamisme économique et social dans les territoires.

Afin de donner de l'écho à ces initiatives, de poursuivre une discussion directe avec les entrepreneurs, et après l'annulation contrainte de l'édition 2020 en raison de la crise sanitaire, la Délégation a donc pu inviter les dirigeants au Sénat le 21 octobre 2021 pour cette cinquième édition de la Journée des Entreprises, qui a réuni 120 chefs d'entreprise venant de plus de 40 départements.

Ils ont débattu, entre eux et avec les sénateurs, de deux sujets ayant fait l'objet de travaux de la Délégation car étant au cœur de l'actualité et des préoccupations des entreprises. Les échanges de la première table ronde ont ainsi porté sur la cybersécurité des entreprises, celle-ci représentant un risque potentiellement mortel pour les entreprises, alors que toutes n'en sont pas suffisamment conscientes ou ne sont pas assez préparées. La seconde table ronde a été consacrée à la prévention en santé et au bien-être au travail ; elle a permis d'échanger sur l'application de la loi du 2 août 2021 pour renforcer la prévention en santé au travail mais aussi sur la nécessaire prise en compte de ces sujets tant par les salariés que par les chefs d'entreprise eux-mêmes.

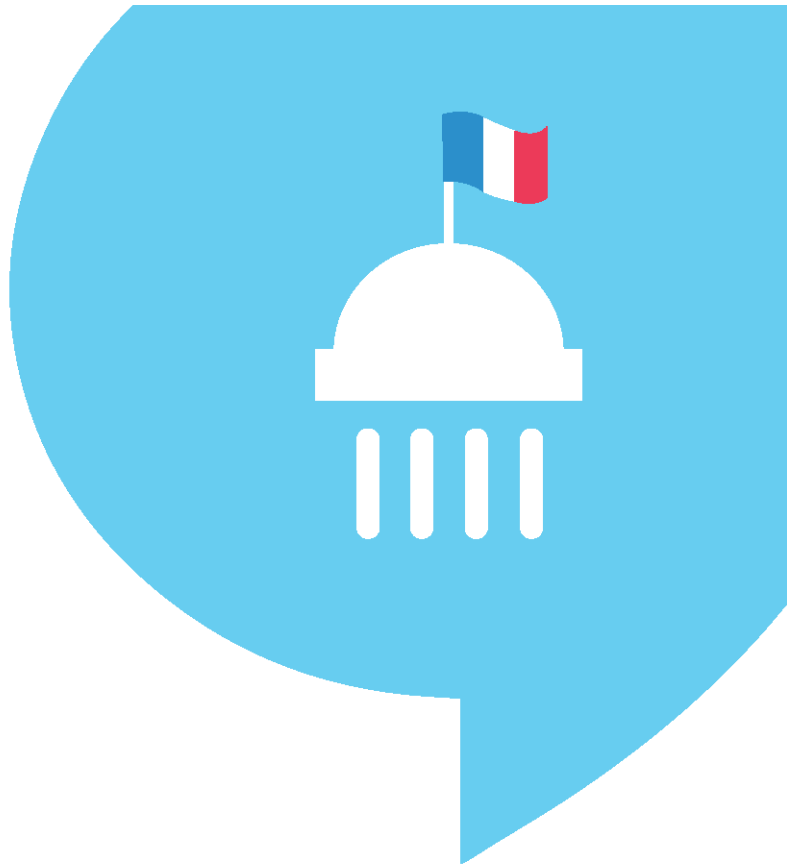
Le présent rapport, qui rassemble le compte-rendu des propos tenus lors des tables rondes de la journée, permet de prendre connaissance de la richesse des échanges intervenus à l'occasion de cette cinquième édition de la Journée des entreprises.

Serge BABARY

Président de la Délégation sénatoriale aux entreprises

PROGRAMME DE LA JOURNÉE





*Le Sénat est heureux de vous accueillir, vous les Chefs d'entreprise venus de toute la France, pour la cinquième édition de la Journée des entreprises, le jeudi 21 octobre 2021. Organisée, au Sénat, par sa Délégation aux entreprises, cette journée est l'occasion de poursuivre le dialogue établi sur le terrain entre sénateurs et dirigeants de PME et d'ETI.*

**Serge BABARY**  
Président de la Délégation aux entreprises





**8h15**

**ACCUEIL - CAFÉ**

**9h**

**OUVERTURE PAR  
M. GÉRARD LARCHER,**  
Président du Sénat.

Introduction des enjeux par  
**M. Serge Babary**, Sénateur, Président  
de la Délégation sénatoriale aux  
entreprises.

**9h15**

**THÈME 1 :  
« LA CYBERSÉCURITÉ DES  
ENTREPRISES ? »**

**TABLE RONDE : « COMMENT  
RÉPONDRE À L'URGENCE ? »**

**Modérateur : M. Emmanuel Cugny**,  
Chroniqueur-éditorialiste à France  
info et Président de l'Association des  
journalistes économiques et financiers.

- > **M. Marc Bothorel**, Membre de la  
commission Numérique de la CPME,  
Associé-gérant de Starware Micro  
Services.
- > **M. Philippe Clerc**, Expert CCI France  
en matière de cybersécurité.
- > **M. Jérôme Notin**, Directeur général de  
cybermalveillance.gouv.fr.
- > **M. Michel Van Den Berghe**, Président  
du Campus cyber, ancien PDG  
d'Orange Cyberdéfense.

**10h25**

**ÉCHANGES AVEC LA SALLE**

**11h15**

**THÈME 2 :  
« PRÉVENTION EN SANTÉ ET  
BIEN-ÊTRE AU TRAVAIL »**

**PRÉSENTATION DES  
ÉVOLUTIONS INDUITES PAR LA  
LOI « SANTÉ AU TRAVAIL »**

- > **Mme Pascale Gruny**, Vice-présidente  
du Sénat, Co-rapporteur de la  
commission des Affaires sociales sur  
la loi du 2 août 2021 pour renforcer la  
prévention en santé au travail

**TABLE RONDE : « QUELS  
OUTILS POUR UN NOUVEAU  
MONDE DU TRAVAIL ? »**

**Modérateur : M. Emmanuel Cugny**,  
Chroniqueur-éditorialiste à France  
info et Président de l'Association des  
journalistes économiques et financiers.

- > **M. Jean-Emmanuel Ray**, Professeur  
de Droit à l'université Panthéon-  
Sorbonne, spécialiste en droit du  
travail.
- > **Mme Amandine Brugière**,  
Responsable du département  
Capitalisation et développement des  
connaissances de l'Agence nationale  
pour l'amélioration des conditions de  
travail (ANACT).
- > **Mme Laurence Breton Kueny**, Vice-  
présidente de l'Association nationale  
des directeurs des ressources  
humaines (ANDRH), Présidente de la  
commission Santé au travail, DRH du  
groupe AFNOR.
- > **Mme Bénédicte Moutin**, Secrétaire  
confédérale de la Confédération  
française démocratique du travail  
(CFDT), en charge du volet Vie au  
travail-dialogue social.

**12h10**

**ÉCHANGES AVEC LA SALLE**

**13h-14h30**

**DÉJEUNER DANS LES SALONS**

**DE BOFFRAND**

Homage aux jeunes champions  
de l'équipe de France *Euroskills 2021*.

**15h**

**FIN DE LA JOURNÉE**

Visite du Sénat par les Sénateurs pour  
les participants intéressés.

*NB : Le passe sanitaire sera demandé pour l'accès au Sénat  
dans le respect des règles sanitaires en vigueur.*

## LES INTERVENANTS



### MARC BOTHOREL

**MEMBRE DE LA COMMISSION NUMÉRIQUE DE LA CPME,  
ASSOCIÉ-GÉRANT DE STARWARE MICRO SERVICES**

Marc Bothorel a réalisé des études d'ingénieur en informatique à Grenoble puis en Californie. En 2007, il a créé sa société StarwareMicro à Saint Michel sur Orge afin d'offrir et de proposer aux particuliers et aux petites et moyennes entreprises des solutions informatiques de proximité et sur mesure, tels que le dépannage, l'assistance, la maintenance, la formation et le conseil. Au travers de son activité, Marc Bothorel s'engage auprès des entreprises à faire de l'outil informatique un avantage concurrentiel pour leur permettre d'être plus efficace, tout en préservant l'intégrité de leurs données vitales et en renforçant la sécurité et la disponibilité des outils de travail informatiques utilisés. Marc Bothorel est aussi l'un des membres de la commission Numérique de la CPME.



### PHILIPPE CLERC

**EXPERT CCI FRANCE EN MATIÈRE DE CYBERSÉCURITÉ**

Philippe Clerc est un ancien élève du Collège d'Europe (Bruges) et des universités de Grenoble, Nanterre, Paris-Dauphine et Kingston-upon-Hull au Royaume-Uni. Après avoir été membre d'un cabinet d'avocat, il a travaillé au sein du Centre des systèmes et technologies avancées (CESTA), au Commissariat général du Plan, au Secrétariat de la Défense nationale et à l'Assemblée des chambres françaises de commerce et d'industrie. Il est nommé conseiller expert en intelligence économique internationale à CCI France en 2013 ainsi que président de l'Académie de l'Intelligence Économique en 2020. En parallèle, il est président l'Association Internationale Francophone d'Intelligence Économique, vice-président du Groupement français de l'industrie de l'information.





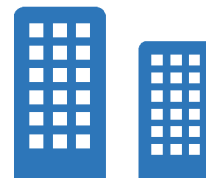
**JERÔME NOTIN**  
**DIRECTEUR GÉNÉRAL DE CYBERMALVEILLANCE**

**Jérôme Notin** a débuté sa carrière dans des entreprises privées liées à la cybersécurité et au logiciel libre. En 2016, il a rejoint l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en tant que préfigurateur d'un dispositif national d'assistance aux victimes d'actes de cybermalveillance. C'est ainsi, qu'il est devenu directeur général dudit dispositif créé en 2017, connu sous le nom de cybermalveillance.gouv.fr, et co-piloté par l'ANSSI et le ministère de l'Intérieur. Son objectif est, d'une part, d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes d'actes de cybermalveillance, et d'autre part, de les prévenir et les sensibiliser aux risques numériques. Pour ce faire, le dispositif met en relation les victimes de cyberattaques avec des prestataires de proximité susceptibles de restaurer leurs systèmes, via une plate-forme numérique. Le dispositif cybermalveillance organise également des campagnes de prévention et de sensibilisation à la sécurité du numérique.



**MICHEL VAN DEN BERGHE**  
**PRÉSIDENT DU CAMPUS CYBER, ANCIEN PDG D'ORANGE CYBERDÉFENSE**

**Michel Van den Berghe** est diplômé de la Faculté polytechnique de Mons. En 2014, sa société Atheos est rachetée par Orange et il devient le directeur d'Orange Cyberdéfense (OCD). Sous son septennat, la filiale s'impose comme le leader européen de la sécurisation informatique. Il a récemment quitté OCD afin de se consacrer pleinement au Campus cyber qu'il a élaboré après avoir été mandaté par le Premier ministre Édouard Philippe. Le Campus accueillera à l'horizon 2022 sur un même site des entreprises (grands groupes, PME), des services de l'État, des organismes de formation, des chercheurs et des associations. L'objectif est de souligner l'expertise de la France en termes de cybersécurité et de construire une société numérique de confiance en créant des synergies afin de lutter contre les cyberattaques et de faire bénéficier aux petites entreprises de véritables moyens de protection.





**JEAN-EMMANUEL RAY**  
**PROFESSEUR DE DROIT À L'UNIVERSITÉ PARIS I**  
**PANTHÉON-SORBONNE, SPÉCIALISTE EN DROIT DU TRAVAIL**

Jean-Emmanuel Ray a réalisé ses études à Sciences Po Paris, à l'Université Panthéon-Assas et à l'Université Panthéon-Sorbonne. Après avoir obtenu son agrégation, il a enseigné le droit du travail à l'Université d'Angers puis à l'Université Panthéon-Sorbonne où il dirige actuellement le Master 2 professionnel « Développement des ressources humaines et droit social ». Il assure également les cours d'introduction générale au droit et de droit du travail à l'IEP de Paris, à Mines ParisTech et au Centre audiovisuel d'études juridiques. En février 2020 il a été nommé par le Premier ministre membre de la « Commission Frouin », chargée de formuler des propositions sur le statut des travailleurs des plateformes. Il assure la chronique « Droit du travail et TIC » pour la revue Droit social, et en alternance « Question de Droit Social » au journal Le Monde.



**AMANDINE BRUGIÈRE**  
**RESPONSABLE DU DÉPARTEMENT CAPITALISATION ET**  
**DÉVELOPPEMENT DES CONNAISSANCES DE L'AGENCE**  
**NATIONALE POUR L'AMÉLIORATION DES CONDITIONS DE**  
**TRAVAIL (ANACT)**

Amandine Brugière a réalisé ses études à l'Université Sorbonne-Nouvelle Paris III, ainsi que dans une école de multimédia, puis à l'Université Paris X Nanterre dans le domaine des sciences de l'information et de la communication. Elle a travaillé à la FING (Fondation Internet Nouvelle Génération) comme Directrice de programme afin d'aider les entreprises, les institutions et les territoires à anticiper les mutations liées aux technologies. Elle a ensuite été sélectionnée pour participer à la 35<sup>ème</sup> session nationale de l'INTEFP (Institut National du Travail, de l'Emploi et de la Formation Professionnelle) organisée par le ministère de l'Emploi, de la formation professionnelle et du dialogue social, sur le thème de la révolution numérique et des nouveaux modèles d'innovation sociale et économique. Elle rejoint enfin l'ANACT en qualité de responsable du département « Études Capitalisation Prospective », puis devient responsable des développements techniques et scientifiques fin 2020.





**LAURENCE-BRETON KUENY**  
**VICE-PRÉSIDENTE DE L'ASSOCIATION NATIONALE DES**  
**DIRECTEURS DES RESSOURCES HUMAINES (ANDRH),**  
**PRÉSIDENTE DE LA COMMISSION SANTÉ AU TRAVAIL,**  
**DRH DU GROUPE AFNOR**

Laurence-Breton Kueny a obtenu son doctorat de Science et Gestion à Bordeaux puis un Master en Management Stratégique des Ressources Humaines à HEC. Elle devient DRH du groupe international AFNOR qui est au service de l'intérêt général et du développement économique. Son objectif est de concevoir et de déployer des solutions fondées sur les normes volontaires, sources de progrès et de confiance autour de quatre grands domaines de compétences : la normalisation, la certification, l'édition de solutions et services d'information technique et professionnelle et la formation. Laurence Breton-Kueny est aussi Vice-Présidente de l'ANDRH depuis 3 ans. C'est une association au service des professionnels des ressources humaines d'entreprises et d'organisations de tous secteurs d'activité et de toutes tailles, publiques et privées, nationales et internationales.



**BÉNÉDICTE MOUTIN**  
**SECRÉTAIRE CONFÉDÉRALE DE LA CONFÉDÉRATION**  
**FRANÇAISE DÉMOCRATIQUE DU TRAVAIL (CFDT), EN CHARGE**  
**DU VOLET VIE AU TRAVAIL-DIALOGUE SOCIAL**

Bénédicte Moutin est prévention santé et sécurité au travail. Son parcours professionnel l'a conduit à s'investir syndicalement dans l'entreprise puis au sein de la CFDT en région Pays de la Loire à la fois sur le territoire de la Mayenne et sur le sujet de la santé au travail. En mars 2016, elle rejoint la confédération CFDT en tant que secrétaire confédérale en charge de l'enquête « Parlons travail » mais aussi des conditions de travail. Aujourd'hui, elle est en charge de la qualité de vie au travail dans une approche élargie au travail qui questionne notamment les organisations et les transformations du travail, le management et le dialogue social.



**M. Emmanuel Cugny, Modérateur, Chroniqueur-éditorialiste à France Info et Président de l'Association des journalistes économiques et financiers**

Bonjour à toutes et à tous. Merci d'être avec nous pour cette grande journée annuelle des entreprises organisée par la DDélégation sénatoriale aux Entreprises. Nous allons dresser un rapide bilan : la vidéo qui suit présente les travaux réalisés par cette importante Délégation du Sénat.

**I. OUVERTURE**

**M. Gérard Larcher, Président du Sénat**

Monsieur le Président de la DDélégation sénatoriale aux Entreprises, cher Serge Babary, je suis très heureux de voir Mme Élisabeth Lamure à nos côtés, car elle a été à l'origine de cette Délégation même si elle me l'attribue.

Je suis heureux de saluer nos collègues sénateurs et élus, la Présidente de la Délégation aux Droits des femmes. Je suis heureux de vous saluer et de vous accueillir, Mesdames et Messieurs les Chefs d'entreprise, Mesdames et Messieurs, pour cette cinquième Journée des entreprises organisée par notre Délégation aux Entreprises. Nous avons créé cette Délégation en 2014 avec la préoccupation d'enrichir les réflexions et les travaux du Sénat par une approche concrète et pragmatique de la vie des entreprises, dans leur diversité et sur le territoire.

Il s'agit d'informer le Sénat sur les situations et les perspectives, notamment de nos PME, d'identifier les obstacles à leur développement et de proposer des évolutions du cadre législatif et réglementaire en s'inspirant de bonnes pratiques et d'expériences locales réussies afin d'encourager la croissance et l'emploi.

Aller à la rencontre des entrepreneurs partout en France et observer le tissu économique local pour mieux comprendre les problématiques de terrain font partie des fondamentaux de la Délégation. Grâce au partenariat que nous avons noué en 2017 avec le réseau des Chambres de commerce et d'Industrie (CCI), les sénateurs qui le souhaitent ont la possibilité de passer un certain nombre de journées en immersion dans des entreprises.

Le président Pierre Goguet nous a rappelé l'intérêt de ces échanges croisés. J'estime qu'ils doivent se poursuivre après la crise sanitaire, car ils représentent le Sénat « dans la vie des entreprises ». Les contacts directs, étroits et approfondis permettent une meilleure compréhension des enjeux économiques locaux et des attentes des entreprises.

La Délégation participe aussi activement aux travaux de contrôle de l'action du gouvernement - l'une des missions essentielles du Parlement, ainsi qu'à l'examen des projets de loi ou des propositions de loi intéressant les entreprises, par le biais des rapports d'information - dont vous avez constaté

le nombre impressionnant depuis la création de la Délégation, des propositions de résolutions, d'amendements ou de propositions de loi.

Je citerai deux exemples. Faisant suite aux retours de terrain récurrents et lancinants, la Délégation a adopté, au printemps 2020, un rapport de M. Michel Canévet et M. Guy-Dominique Kennel relatif au manque de compétences et aux difficultés de recrutement dans un contexte de forte évolution des métiers.

Ce rapport et les recommandations qu'il contient me semblent être au cœur de l'actualité. Alors que la France enregistre toujours le cinquième taux de chômage le plus élevé de l'Union européenne, plusieurs centaines de milliers d'emplois ne sont pas pourvus et une proportion croissante d'entreprises, notamment de l'industrie et du bâtiment, ne trouvent pas les compétences dont elles ont besoin.

Je rencontre ce problème majeur dans tous les départements. Nous ne pouvons pas nous satisfaire d'un taux de chômage structurel qui stagne autour de 7 %, alors que celui de nos voisins avoisine les 3,5 %. J'estime ce sujet essentiel pour relancer vraiment l'économie. Les plans de relance ne peuvent donner de résultats satisfaisants sans les femmes et les hommes pour les réaliser.

Un autre exemple concret concerne l'évolution des modes de travail : je pense à l'essor du télétravail, à la fragmentation des parcours professionnels, au développement des microentreprises et à l'apparition de nouvelles formes d'emploi à la frontière entre travail indépendant et salariat. Nous constatons aussi cette évolution dans des débats sociaux actuels.

Le rapport d'information présenté par Mme Martine Berthet, M. Michel Canévet et M. Fabien Gay a analysé tous ces phénomènes qui transforment profondément le monde du travail. Ils constituent un véritable défi pour les *managers* et les chefs d'entreprise. Ils sont aussi porteurs de nouveaux risques pour les travailleurs, auxquels nous devons être attentifs.

Nous devons être attentifs à ces points très concrets, y travailler et les partager avec vous.

L'édition 2020 de la journée des entreprises a malheureusement été annulée pour des raisons de crise sanitaire. Malgré ce contexte, le dialogue établi sur le terrain entre les sénateurs et les entreprises s'est poursuivi sous d'autres formes grâce à l'engagement personnel de Mme Élisabeth Lamure puis de M. Serge Babary.

La Délégation a maintenu régulièrement informés les sénateurs ainsi que les acteurs locaux soucieux d'orienter les entreprises vers les mesures mises en place pour les aider à traverser la crise. Je rappelle que le Sénat a soutenu le dispositif d'activité partielle, le Fonds de solidarité, les prêts garantis par l'État ou les aides à la numérisation des TPE, PME et ETI.



La Délégation s'est également mobilisée au service de toutes les entreprises du pays en relayant leurs craintes, leurs difficultés et leurs attentes, ainsi que les initiatives et les bonnes pratiques mises en place dans les territoires.

Les entreprises ont traversé une période particulièrement difficile, car totalement inédite et imprévisible. Grâce aux mesures d'urgence déployées par l'État et apportées par les collectivités territoriales, les entreprises ont plutôt bien résisté : de nombreuses faillites ont été évitées et l'emploi a été globalement préservé.

Confrontées à un contexte évolutif et incertain, les entreprises semblent avoir fait preuve d'une grande agilité et ont su adapter en permanence leur mode d'organisation et de fonctionnement : le télétravail s'est développé par la force des circonstances ; la digitalisation et la numérisation des entreprises, qui doivent renforcer leur compétitivité et ouvrir de nouvelles perspectives, se sont accélérées.

Une traduction visible en a été l'essor significatif du e-commerce sous différentes modalités (la vente en ligne sur les plateformes spécialisées ou directement sur le site des entreprises) : en 2019, il représentait 9 % du commerce de détail ; aujourd'hui, 13 %. Cette augmentation de 30 % doit nous amener à réfléchir sur un certain nombre de modes d'organisations.

Cette crise sanitaire a accéléré ces évolutions et ouvert de nouvelles opportunités. Elle a également mis en lumière de nouvelles fragilités. Ce matin, vos débats porteront sur deux d'entre elles : la cybersécurité et la santé au travail.

La cybersécurité sera l'objet de la première table ronde. La cybercriminalité peut être mortelle pour les entreprises, notamment les PME. La généralisation des usages du numérique (internet des objets, e-commerce et télétravail) s'accompagne d'une hausse vertigineuse des actes de piratage, sous forme de rançonnage numérique essentiellement.

Les collectivités territoriales n'y échappent pas. Je ferai prochainement un point avec le patron de la Gendarmerie nationale, car les situations sont comparables. Les rançonneurs numériques sont nombreux et présents.

Actuellement, des centaines d'entreprises sont quotidiennement victimes de telles attaques, qui consistent à bloquer leur système informatique et à exiger une forme de rançon pour débloquer les données. Les entreprises doivent donc mettre en place des mesures de protection efficaces et les adapter en permanence à une menace évolutive toujours plus sophistiquée qui se professionnalise et s'internationalise.

Dès le mois de février, cher Président, la Délégation que vous présidez a lancé une mission relative aux enjeux de cybersécurité dans les entreprises. À l'issue de ses travaux ponctués par plusieurs tables rondes, visites sur le terrain et auditions, elle a adopté à l'unanimité le rapport de M. Sébastien

Meurant et M. Rémi Cardon afin de mettre en place plusieurs propositions pour que la cybersécurité soit à la portée de toutes les entreprises.

Je crois que vos échanges de ce matin permettront de poursuivre la réflexion sur les dispositifs à mettre en place en matière de prévention, de protection publique et privée, de prise en charge des victimes et de répression de la cybercriminalité. Actuellement, notre commission des lois tient une série de rencontres et d'agoras avec la justice. Aussi, nous devons sensibiliser l'autorité judiciaire à ces réalités.

Notre seconde table ronde, qui ne peut qu'être chère à un ancien ministre du Travail, sera consacrée à la prévention et au bien-être au travail. Ce thème n'est pas totalement délié des problèmes de recrutement et de ressources humaines que j'ai précédemment évoqués.

En 2005, le premier plan de santé au travail reposait sur une approche positive du travail et visait à réconcilier progrès économique et progrès social. La société de participation peut apporter une réponse à la crise sociale et sociétale que notre pays traverse. Les chefs d'entreprise et les responsables politiques doivent partager cet objectif de société, car une économie compétitive permet aussi à ses salariés de se réaliser au travail.

Mme Pascale Gruny, notre Vice-Présidente, vous présentera la loi d'août 2021 pour renforcer la prévention au travail dont elle a été le co-rapporteur avec M. Stéphane Artano qui préside notre Délégation aux Outre-mer.

Issu d'un accord national interprofessionnel, ce texte est la manifestation de la vitalité du dialogue social, enclenché par les partenaires sociaux eux-mêmes, et de l'intérêt accru porté aux conditions de travail. Il devrait permettre d'afficher une véritable priorité en faveur de la prévention des accidents du travail et des maladies professionnelles. Il améliorera également les dispositifs existants en matière de gouvernance et d'offre des services de santé au travail, notamment concernant les PME. Enfin, il garantira un meilleur accompagnement des publics les plus vulnérables. Il constituera, nous l'espérons, une réelle avancée de nature à mieux intégrer les actions de santé au travail dans la politique générale de santé publique.

Le Sénat porte une attention particulière à la vie et au développement des entreprises, car elles sont au cœur de la vie de nos territoires. Notre assemblée représente l'ensemble des territoires (urbains, ruraux et ultramarins) dont l'activité est en grande partie structurée par nos entreprises. Elles font la force de notre pays, à la fois solidaire et productif.

Recenser les obstacles à leur développement et proposer les mesures favorisant l'esprit d'entreprise, la croissance et l'emploi : telle est la raison d'être de notre Délégation.

Je sais que le président Babary et les sénateurs de la Délégation veilleront à ce que les idées que vous ferez éclore soient intégrées et suivies

d'actions concrètes. Les délégations ne sont nullement en concurrence avec les commissions : elles apportent une ouverture et une réflexion supplémentaire. Je crois vraiment au rôle des délégations dans la vie de notre Sénat et dans la vie politique de notre pays.

Je vous souhaite une très bonne journée.

### **M. Serge Babary, Président de la Délégation aux entreprises**

Monsieur le Président, cher Gérard, mes chers collègues, Mesdames et Messieurs, ces quelques mots d'accueil pour vous dire combien nous nous réjouissons de renouer avec notre journée des entreprises, dont c'est aujourd'hui la cinquième édition.

Alors que cette dernière devait se dérouler le 2 avril 2020, la brutale crise sanitaire nous avait contraints à la reporter. Le Sénat est donc heureux de vous accueillir aujourd'hui. Vous êtes près de 150 chefs d'entreprise venus de plus de 40 départements. Vous incarnez donc le dynamisme économique des territoires français que vient de rappeler notre Président.

Organisée par la DDélégation sénatoriale aux Entreprises, cette journée est l'occasion de poursuivre le dialogue établi sur le terrain entre sénateurs et dirigeants de PME et d'ETI. Créée fin 2014 à l'initiative du Président du Sénat, cette Délégation qui rassemble 42 sénateurs de toutes sensibilités politiques est chargée d'informer le Sénat sur la situation des entreprises, de recenser les obstacles à leur développement et de proposer des mesures visant à favoriser l'esprit d'entreprise et à simplifier les normes applicables à l'activité économique en vue d'encourager la croissance et l'emploi dans nos territoires.

Malgré une interruption des déplacements liée à la pandémie, la Délégation a rencontré des centaines d'entrepreneurs français dans 32 départements. Sur le fondement de témoignages de terrain ainsi recueillis, elle agit de différentes manières : interpellations et questions au gouvernement, amendements, propositions de loi, propositions de résolutions et rapports pour informer et préconiser des solutions sur des sujets importants pour la vie des entreprises de la Nation.

Cette année, outre le suivi des modalités et conditions de la reprise concrète de l'activité économique, nous avons travaillé sur les deux thèmes qui feront l'objet de nos débats de ce jour.

La cybersécurité des entreprises a fait l'objet du rapport de nos collègues M. Sébastien Meurant et M. Rémi Cardon « *Prévenir et guérir. Quels remèdes contre les cybervirus ?* » Elle représente en effet un risque potentiellement mortel pour les entreprises et toutes n'en sont pas suffisamment conscientes. En ce mois d'octobre, mois de la cybersécurité, nous espérons que nos travaux contribueront à faire avancer ce sujet majeur.

La prévention en santé et le bien-être au travail a fait l'objet du rapport de nos collègues Mme Martine Berthet, M. Michel Canévet et M. Fabien Gay « *Évolution des modes de travail, défis managériaux : comment accompagner entreprises et travailleurs ?* » Ce sujet est plus que jamais d'actualité. Les échanges pourront aussi porter sur l'application de la loi du 2 août 2021 pour renforcer la prévention en santé au travail.

Cette préoccupation concerne tous les salariés, mais également tous les dirigeants. Cette journée sera un moment fort de ce qui fait l'ADN de la Délégation que j'ai l'honneur de présider. Afin que le dialogue avec les entreprises se poursuive au-delà de notre rendez-vous annuel, n'hésitez pas à nous contacter pour nous faire part d'éventuelles difficultés liées à l'application concrète de textes législatifs ou réglementaires. Je vous assure de la pugnacité des 42 membres de notre Délégation pour prendre en compte vos remarques et les porter au niveau des ministères.

Notre mobilisation en faveur de la simplification de la vie des entreprises guidera toujours notre action, quelle que soit la source de complexité ou de difficulté.

Je donne maintenant la parole à M. Emmanuel Cugny, notre modérateur, que je remercie ainsi que vous tous pour votre présence et votre participation. Très bonne journée à tous.

## II. THÈME 1 : LA CYBERSÉCURITÉ DES ENTREPRISES

### A. TABLE RONDE : « COMMENT RÉPONDRE À L'URGENCE ? »

#### M. Emmanuel Cugny

Merci Monsieur le Président de la Délégation sénatoriale aux entreprises.

Je vous propose de commencer cette première table ronde. L'urgence est celle de maîtriser le monde d'après-crise et de protéger l'entreprise face aux attaques informatiques de prédateurs puissants. Les solutions sont nombreuses : encore faut-il les connaître et se les approprier.

M. Bothorel, où en sont les PME aujourd'hui en matière de défense contre la cybercriminalité ? Contrairement à des idées reçues, les PME-PMI sont visées, comme les grands groupes. Or, les dirigeants n'en ont pas véritablement conscience.

#### M. Marc Bothorel, Référent cybersécurité de la CPME, Associé-gérant de Starware Micro Services

Je suis très heureux d'être avec vous aujourd'hui et de représenter la CPME, organisation patronale réunissant 244 000 entreprises

Je rappellerai d'abord quelques éléments chiffrés. La

Les attaques augmentent, avec notamment + 400 % sur les rançongiciels selon l'ANSSI). La gestion de crise est problématique en France, car les TPE-PME ne souhaitent pas toujours partager leur expérience pour ne pas inquiéter leurs clients.

Par ailleurs, la Fédération Française des Assurances (FFA) considère depuis deux ans que le risque « cyber » est le premier risque que les entreprises doivent assurer sur les cinq prochaines années.

Ces informations apparaissent suffisamment inquiétantes pour que la CPME s'empare du sujet. Nous sommes engagés depuis de nombreuses années dans la sensibilisation des dirigeants de PME, car ils persistent à croire que les cybercriminels ne s'intéressent qu'aux grosses entreprises.

Depuis le début de la crise, nombre de nos adhérents ont digitalisé leur entreprise : certains y ont été forcés ; d'autres ont installé dans l'urgence une structure de télétravail. Pour autant, ils n'ont pas modifié leur périmètre de sécurité existant. Certains se sont retrouvés isolés et affaiblis dans un contexte anxiogène - terrain fertile des cybercriminels. Ils ont parfois autorisé l'utilisation du matériel personnel, non protégé.

Or, la voie royale qu'empruntent aujourd'hui les *hackers* est le poste de travail : 80 % des attaques réussies commencent par une attaque de type *phishing* pour extorquer des informations ou implanter un *malware*.

Nous répétons que la transformation numérique est obligatoire pour assurer la survie des entreprises. Néanmoins, une transformation digitale réussie ne peut s'effectuer sans une composante « cyber » forte qui permet de protéger les données.

La mission de la CPME consiste à protéger les entreprises et diminuer le risque d'attaques. Nous prônons la sensibilisation, notamment au travers du guide que nous avons édité en 2015 et que nous avons revu depuis. Une nouvelle version devrait être publiée en 2022. Elle s'appuie sur douze bonnes pratiques, simples, d'hygiène informatique, qui permettent de diminuer sensiblement la surface d'attaque.

Une étude récente d'IDC montre que la sensibilisation régulière des employés dans le cadre d'un plan de formation diminue les risques « cyber » d'au moins 40 %.

La protection relève aussi d'autres mesures. Je suis notamment satisfait du réseau d'alertes mis en place récemment. Beaucoup d'éléments se mettent en place, mais les chefs d'entreprise doivent encore être convaincus que le futur monde numérique est dangereux. La cybercriminalité est une économie souterraine très bien organisée. Nous devons joindre nos efforts pour la combattre.

### **M. Emmanuel Cugny**

Vous réalisez un travail quotidien minutieux. Nous aurons l'occasion de revenir sur la cybersécurité des PME.

M. Philippe Clerc, l'enquête régionalisée qu'a menée CCI France sur les difficultés rencontrées par les entreprises en matière de cybercontrôle a révélé de sérieuses lacunes.

### **M. Philippe Clerc, Expert CCI France en matière de cybersécurité**

Je vous remercie infiniment pour cette invitation. Effectivement, la riposte à cette pandémie de cybercriminalité nécessite un travail collectif et des partenariats consolidés entre toutes les institutions et les entreprises.

L'objectif prioritaire des CCI est d'accompagner le développement des entreprises sur l'ensemble de nos territoires. En matière de cybersécurité, il est essentiel d'enquêter, de suivre l'évolution de la menace et d'étudier la sociologie et les modalités d'intervention des cybercriminels qui se professionnalisent et intègrent l'économie réelle.

Au fil des mois, nous constatons l'ampleur de la menace. La pandémie a considérablement accéléré la transformation digitale des pratiques, y compris au sein des TPE. En parallèle, la cybercriminalité s'accroît. Or, nous prenons chaque jour du retard dans la riposte, la sensibilisation et l'accompagnement. Face à cette menace, nous devons donc réarmer les territoires.

Nos enquêtes révèlent régulièrement que nos PME considèrent la menace « cyber » comme prioritaire. Une enquête récente relative au partage des données industrielles, sur lequel repose l'avenir du système productif par l'intégration des petites entreprises sous-traitantes, révèle que les principaux freins des PME sont la cybersécurité et la qualité des données. Cet enjeu de compétitivité est important dans le nouveau modèle productif qui se met en place à travers la digitalisation et la transition écologique.

Les PME ne comprennent pas la complexité technologique et n'ont pas les moyens suffisants pour investir considérablement dans les outils et les procédures d'intervention que permettent les institutions.

Enfin, je salue le rapport que vous avez publié, car il sert de support aux CCI pour engager des procédures de sensibilisation et mobiliser les entreprises.

**M. Emmanuel Cugny**

Parmi les outils proposés aux chefs d'entreprise pour lutter contre la cybercriminalité, la prise en compte des dangers fait défaut depuis le début de la pandémie. M. Jérôme Notin, pourriez-vous nous présenter votre mission et *cybermalveillance.gouv.fr* ?

**M. Jérôme Notin, Directeur général de *cybermalveillance.gouv.fr***

*cybermalveillance.gouv.fr* est une plateforme qui permet aux chefs d'entreprise de trouver une solution lorsqu'ils sont victimes d'un acte de cybermalveillance qu'ils ne sont pas capables de qualifier.

La plateforme propose un rapide parcours : elle pose un diagnostic grâce aux réponses à quelques questions et donne les conseils qui permettront à la victime de résoudre sa problématique. Elle est un guichet unique et oriente éventuellement vers un service existant de l'État, comme Perceval, Thésée ou Pharos. Enfin, la plateforme apporte des conseils techniques et propose la mise en relation avec des prestataires de proximité. 1 200 prestataires sont aujourd'hui capables d'aider, sur l'ensemble du territoire national, nos chefs d'entreprise, nos patrons de collectivités, voire les particuliers lorsqu'ils subissent un incident, notamment en raison de rançongiciels, ces virus qui bloquent les systèmes d'information des entreprises et des collectivités.

La plateforme a été créée en 2017 par l'ANSSI et le ministère de l'Intérieur. Elle identifiait alors des prestataires référencés. Depuis début 2021, un label « ExpertCyber » permet aux chefs d'entreprise d'identifier les prestataires qui ont une expertise en remédiation et la capacité d'assister les dirigeants dans la sécurisation de leur système d'information à titre préventif.

Les besoins de prévention et de sensibilisation ont été largement évoqués. Depuis le début du dispositif, nous avons produit beaucoup de

contenus de sensibilisation. En 2020, nous avons diffusé des vidéos sur les chaînes des groupes TFI et Canal afin d'encourager la prise de conscience du risque.

Cette première étape semble en partie franchie aujourd'hui. Elle permettra ensuite d'adresser le risque, car nous offrirons aux entreprises les possibilités de se sécuriser par des contenus de sensibilisation ou des approches techniques comme la diffusion des coordonnées des prestataires locaux.

Enfin, la mise en place d'un observatoire de la menace nous permet de faire connaître notre dispositif, de produire nos propres chiffres - nous avons notamment observé la tendance de l'évolution des rançongiciels entre 2018 et 2020 - et de collecter différentes informations de nos membres (les ministères, la CPME, les CCI, le MEDEF, France Victimes et les entreprises privées) pour évaluer le coût économique de la cybermalveillance.

### **M. Emmanuel Cugny**

Vous êtes tous les témoins de cette nécessaire coordination dont nous aurons l'occasion de débattre. M. Michel Van Den Berghe, vous avez été nommé par le Premier ministre Édouard Philippe : pourriez-vous nous présenter le Campus Cyber ?

### **M. Michel Van Den Berghe, Président du Campus Cyber, ancien PDG d'Orange Cyberdéfense**

Ce projet a effectivement été initié par le président de la République afin de rassembler l'ensemble de l'écosystème de la cybersécurité au sein d'un lieu emblématique. Campus Cyber vise quatre objectifs.

#### **1. Mieux protéger l'économie numérique en s'appuyant sur une expertise collective**

Ce campus sera d'abord un lieu d'opérations. Tous les acteurs de la cybersécurité y déporteront tout ou partie de leurs experts en cybersécurité informatique. 1800 experts intégreront le Campus Cyber pour mieux servir les petites et les grandes entreprises françaises.

#### **2. Promouvoir l'excellence française en matière de cybersécurité**

Nous souhaitons montrer que nous sommes l'un des premiers pays experts en cybersécurité et que nous pouvons être *leader* dans certains domaines du numérique, notamment la cybersécurité.

#### **3. Rapprocher la recherche, l'innovation et l'industrie**

L'enjeu est de faire émerger les licornes de demain et de les conserver. L'INRIA, le CNRS, le CEA, et les ministères de l'Économie et de la Recherche planteront également des chercheurs sur ce campus.

2 000 mètres carrés seront ainsi dédiés à la recherche et plus de 30 *start-up* s'y installeront.



#### 4. Pallier le manque d'expertise en matière de cybersécurité

Nous risquons de souffrir rapidement d'un manque d'experts pour protéger les entreprises. C'est pourquoi nous devons créer un lieu qui modifie l'image de la cybersécurité.

Aujourd'hui, les jeunes ne sont pas attirés par ce métier. Nous avons mené une étude avec le rectorat d'Île-de-France : quand 15 000 jeunes sont formés aux métiers du numérique, seuls 100 s'orientent vers les métiers de la cybersécurité, car ils sont méconnus et souffrent d'une image négative (le « geek à capuche »). Parmi les métiers de la cybersécurité, certains relèvent pourtant de la communication et requièrent de connaître la sensibilité de l'entreprise pour bien la protéger.

L'image de ces métiers doit donc être renouvelée et féminisée - moins de 8 % de femmes exercent un métier dans le domaine de la cybersécurité. Ce campus a vocation à devenir un *show-room* destiné à promouvoir l'image de la cybersécurité, essentielle à la transformation numérique des entreprises.

Le président de la République avait souhaité que le campus soit une initiative privée soutenue par l'État. Nous avons donc créé une SAS qui compte aujourd'hui plus de 100 actionnaires privés : de grandes entreprises comme BNP, Total, LVMH ou L'Oréal ont investi dans des actions du campus ; l'État a abondé à hauteur de 3,5 millions d'euros par l'intermédiaire de l'agence des participations de l'État. Nous avons donc un capital de 8 millions d'euros pour démarrer cette entreprise.

Les futurs résidents avaient demandé que le projet ne se transforme pas en un projet d'aménagement du territoire, car cet écosystème extrêmement sensible manque de ressources. Nous avons donc choisi d'implanter Campus Cyber à Puteaux, à proximité de la station de RER, du métro et du T2, pour pouvoir accueillir les experts en cybersécurité. Une tour de 26 000 mètres carrés ouvrira ses portes en février. Ce campus est un vrai succès aujourd'hui : des acteurs comme la DGSE, l'ANSSI, [cybermaveillance.gouv.fr](http://cybermaveillance.gouv.fr), le ministère de l'Intérieur ou le ministère de la Défense y implanteront des experts.

Ce projet est soutenu au plus haut niveau de l'État. Nous serons donc aidés pour créer les solutions permettant de mieux protéger les entreprises, notamment les plus petites. Aujourd'hui, les patrons de PME sont souvent démunis, car ils n'ont pas de directeur de la sécurité informatique (DSI). Nous souhaitons donc créer des solutions très simples à installer en rassemblant les petites et les grandes entreprises.

Dans le cadre du plan d'action « cyber » qui a été annoncé par le président de la République, 1,1 million d'euros seront consacrés au Campus Cyber pour créer des solutions communes. La région Île-de-France nous a donné une subvention de 2 millions d'euros ; la BPI financera également des projets sur ce campus à hauteur de quatre millions d'euros.

Plusieurs groupes de travail ont commencé leurs réflexions sur la formation, l'anticipation et la sécurisation des cryptomonnaies. Plus de 80 entreprises travaillent déjà ensemble de façon virtuelle sur le Campus Cyber.

Mon objectif est d'en faire une sorte de « porte-avions numérique » de la sécurité française : un porte-avions est grand, dissuasif, fonctionne grâce à la coordination de tous et permet de faire décoller des avions de chasse. Je souhaite tout le succès à ce Campus Cyber national pour ne plus entendre que les Américains font mieux que nous.

## **B. DÉBAT**

### **M. Emmanuel Cugny**

Quel calendrier prévoyez-vous jusqu'à la phase opérationnelle ?

### **M. Michel Van Den Berghe**

Nous prévoyons de faire arriver les premières équipes début février 2022. La crise sanitaire a freiné l'approvisionnement de certains matériels, comme les prises réseau.

L'inauguration par le président de la République ainsi que l'accueil de quelques délégations dans le cadre de la présidence française de l'Union européenne sont prévus au mois de février.

### **M. Emmanuel Cugny**

À vous entendre, M. Philippe Clerc, nous avons l'impression de voir la menace « cyber » comme l'autre pandémie. La cybercriminalité suit elle directement la crise sanitaire ?

### **M. Philippe Clerc**

Le nombre des attaques est suivi par l'observatoire et le nombre d'alertes, recueilli par les CCI. L'accélération de la digitalisation encourage les cybercriminels à attaquer le « maillon faible » du système productif : les TPE, les PME et les sous-traitants.

Or, la digitalisation accélérée concerne tout le système productif. À court terme, les petites entreprises et toutes les compétences alimenteront des plateformes industrielles. Toutes nos PME évoluent dans un écosystème qui sonde la sécurisation, car les menaces se transmettent comme des virus.

### **M. Emmanuel Cugny**

Comment pouvons-nous anticiper ce phénomène ?

### **M. Philippe Clerc**

Le directeur de l'ANSSI évoque souvent ce facteur essentiel sur lequel nous devons nous mobiliser. L'année dernière, les CCI ont étudié la cyberrésilience.

Aujourd'hui, la cybersécurité est traitée et prise en charge : la mobilisation est engagée, mais nous n'anticipons pas suffisamment. Comme en matière de gestion de crise, nous devons tous ensemble préparer toutes nos entreprises à la résolution de la menace.

Dans les chambres de commerce, nous avons formé 18 cyberréférents. Leurs compétences sont certifiées : ils maîtrisent l'écosystème d'intervention et peuvent intervenir auprès des entreprises pour comprendre la menace qui leur est adressée, les aider et les orienter.

Anticiper consiste finalement à préparer toutes nos entreprises à la résolution de la menace en intégrant ces questions de cybersécurité, car la cybercriminalité n'est pas la préoccupation prioritaire des chefs d'entreprise qui gèrent leur carnet de commandes, survivent dans la crise et préparent les futures innovations.

### **M. Emmanuel Cugny**

Pourtant la cybermalveillance est l'affaire de tous....

### **M. Philippe Clerc**

Le risque est désormais connu. La communication est établie sur le sujet.

Anticiper consiste aussi à aider le chef d'entreprise à intégrer les problématiques et le coût de la cybersécurité dans son modèle d'affaires, lequel évolue en fonction de la transition généralisée du système productif et des modes de consommation.

Au demeurant, la cybersécurité ne représente pas un coût, mais un investissement, une assurance-vie pour l'entreprise.

### **M. Emmanuel Cugny**

Comment les patrons de PME peuvent-ils intégrer ce risque aujourd'hui ? Lors des événements de *Cyber October* organisés par Bercy, j'ai été frappé de rencontrer des chefs d'entreprise qui pensaient n'être jamais confrontés à ce risque. En prennent-ils davantage conscience ?

### **M. Marc Bothorel**

J'estime en effet que la crise sanitaire a accéléré la prise de conscience pour deux raisons :

#### **La première est l'augmentation phénoménale du nombre d'attaques**

Lors des séminaires de sensibilisation que j'anime souvent avec M. Jérôme Notin, je présente des cartes interactives d'attaques. Certains acteurs de la cybercriminalité ont décuplé leurs attaques quotidiennes dans le monde.

Nous pouvons qualifier cette évolution de pandémie. Elle produit des milliers de variants quotidiens, mais nous n'avons malheureusement pas de vaccin.

Nous observons parfois des failles de sécurité qui ne sont pas corrigées immédiatement par les éditeurs ou les constructeurs. Elles sont susceptibles de représenter une menace importante pour les entreprises.

Cette pandémie n'est pas terminée. Les cybercriminels travaillent entre eux, parfois avec l'appui de certains gouvernements. Nous devons, nous aussi, unir nos efforts face à cette menace.

#### **La seconde raison est que la communication des chefs d'entreprise s'est améliorée.**

Les dirigeants partagent leur expérience, notamment lors de réunions organisées par la CCI ou la CPME. Ils commencent à réaliser que les petites entreprises sont également visées par la cybermalveillance. Elles peuvent être les victimes collatérales d'attaques de grande ampleur ou représenter des vecteurs d'attaques d'importants donneurs d'ordre.

### **M. Emmanuel Cugny**

Elles ressemblent à un cheval de Troie.

### **M. Marc Bothorel**

Toute la chaîne économique est ainsi mise en danger. Nous observons une certaine latence, mais je me réjouis que la crise sanitaire fasse prendre conscience aux entreprises de la létalité du risque « cyber ».

### **M. Emmanuel Cugny**

La cybersécurité est-elle vraiment coûteuse ?

### **M. Marc Bothorel**

La dépense en cybersécurité n'a pas vocation à être rentable. Elle représente un investissement, voire une assurance, au même titre que la responsabilité civile. Elle permet de garantir aux clients et aux donneurs d'ordre que la relation commerciale et industrielle est protégée.

Par analogie, le Règlement général sur la protection des données (RGPD) permet d'assurer aux partenaires de l'entreprise que leurs données personnelles sont protégées. Il doit être envisagé comme un atout commercial plutôt que comme une punition.

La protection ne coûte pas nécessairement cher. Au demeurant, le système pourrait ne pas être protégé, à condition que les sauvegardes régulières permettent de le réinstaller rapidement en cas d'attaque.

### **M. Jérôme Notin**

Cette salle est équipée d'un dispositif anti-incendie et d'extincteurs qui permettent d'arrêter un départ de feu le cas échéant. Quelle qu'elle soit, la protection est un investissement fondamental.

Aujourd'hui, des entreprises déposent leur bilan à cause de cyberattaques. Pour éviter de mourir, il apparaît donc judicieux de consacrer un pourcentage raisonnable de son chiffre d'affaires à la cybersécurité. Elle n'est d'ailleurs pas nécessairement onéreuse.

Nous avons imaginé le dispositif « Alerte Cyber » avec le MEDEF, la CPME, l'U2P et l'ANSSI pour informer des vulnérabilités critiques que nous avons identifiées grâce à notre veille. Nous rédigeons un courriel simple à destination des chefs d'entreprise et utilisons les canaux du MEDEF, de la CPME et de l'U2P pour toucher 80 à 95 % des entreprises. Nous présentons la menace et la solution technique.

Les Britanniques ont compris qu'en élevant légèrement le niveau de sécurité global du pays, les cybercriminels, qui sont fainéants, se tourneraient vers d'autres pays. Les entreprises ont intérêt à s'inspirer de ce raisonnement : à terme, le niveau de sécurité de toutes nos entreprises s'élèverait.

### **M. Emmanuel Cugny**

Quelles actions (sensibilisation, formation) l'entreprise peut-elle envisager en interne ?

### **M. Michel Van Den Berghe**

Depuis des années, les entreprises multiplient les équipements de cybersécurité. Le marché de la cybersécurité est en forte croissance, mais les entreprises ne sont pas forcément protégées. Elles doivent d'abord envisager un « plan B ».

La sauvegarde externe permet à l'entreprise de sécuriser ses données et de limiter ses pertes. Il faut revenir à beaucoup de bon sens.

Cet été, Orange est beaucoup intervenue auprès des hôpitaux. Lorsqu'ils sont attaqués, les patients ne sont plus soignés. Les experts en cybersécurité s'occupent alors de récupérer les dossiers numériques des patients qui contiennent toutes les données permettant de les soigner.

La cybersécurité devient extrêmement sensible et doit être gérée avec beaucoup de bon sens.

**M. Emmanuel Cugny**

Quels sont les gestes simples du quotidien ?

**M. Michel Van Den Berghe**

Il convient de porter la même attention aux courriers électroniques qu'aux courriers postaux : vous n'envoyez pas votre numéro de carte bleue à quelqu'un que vous ne connaissez pas et qui vous a écrit pour vous demander de l'argent.

**M. Marc Bothorel**

Il convient effectivement d'appliquer les principes de précaution de la vie réelle à la vie numérique.

Pour une TPE de dix personnes, une enveloppe de 5 000 euros annuels permet de financer les éléments fondamentaux de protection technique (*antimalware*, *antispams*, pare-feu et sauvegarde). Cette somme est à envisager au regard du temps de restauration des données et des effets connexes de réputation.

**M. Emmanuel Cugny**

Comment attirer les jeunes vers les métiers de la cybersécurité ?

**M. Michel Van Den Berghe**

Nous devons générer des vocations et créer l'attractivité autour des métiers de la cybersécurité en changeant leur image. Cette activité a autant de sens que celle des pompiers : il s'agit d'éteindre le feu.

La sûreté d'un véhicule est devenue un critère de choix qui pourrait aussi convenir aux applications informatiques. Nous avons besoin de communication et de pédagogie. Enfin, nous devons féminiser nos métiers et améliorer l'image des experts en cybersécurité qui ne sont pas tous des « *geeks* à capuche ».

**M. Emmanuel Cugny**

Quel est le positionnement des CCI sur le terrain ?

**M. Philippe Clerc**

Dans le réseau des CCI, l'Institut Méditerranéen d'Etudes et Recherche en Informatique et Robotique (IMERIR) forme à la cybersécurité dans le domaine de la robotique et de l'intelligence artificielle. Nous avons besoin de compétences supplémentaires.

Par ailleurs, j'insiste sur la transversalité du métier : aujourd'hui, la cybersécurité devient un élément de la sécurité globale. Les responsables de la cybersécurité doivent communiquer sur cette caractéristique, car ils doivent gérer un déséquilibre permanent avec des pics de crise.

### **M. Emmanuel Cugny**

M. Jérôme Notin a évoqué cet objectif commun auquel chacun doit contribuer, chefs d'entreprise et parlementaires. Nous passons aux questions de la salle.

Nous avons constaté lors de la pandémie que les pertes d'exploitation des restaurateurs n'étaient pas prévues par les grands assureurs. Le risque cyber est-il réellement couvert par les assureurs ?

### **M. Guillaume Cochet, CMPE Rhône, Président de la chambre professionnelle des agents généraux d'assurance du Rhône, Vice-Président de l'association interprofessionnelle des assureurs lyonnais**

80 % des entreprises sont touchées par le cyberrançonnage, que nos contrats couvraient. Or, le Sénat a très fortement préconisé aux assureurs de supprimer cette garantie pour ne pas financer le cyberterrorisme.

Pourtant, j'estime important de prendre en compte le risque légal pour les entreprises et d'enquêter à l'international, car les vrais acteurs se situent en dehors de la France (Israël, Europe de l'Est...).

Dans ce contexte, les assurances ne disposent pas de moyens suffisants pour proposer des solutions pertinentes à 80 % des entreprises alors qu'elles ont vocation à les sensibiliser. Les propositions actuelles concernent 20 % des entreprises et se limitent à couvrir la perte d'exploitation, les dommages matériels et la reconstitution de données logiques.

### **M. Jérôme Notin**

Le Sénat a en effet préconisé d'interdire le paiement des rançons. En tant que citoyen, j'estime cette position intelligente, judicieuse et pragmatique. Les assureurs ont vocation à imaginer des solutions de prévention.

### **M. Guillaume Cochet**

Le terrorisme ne sera pas asséché, car les cybercriminels trouvent suffisamment de ressources auprès des entreprises, en France et ailleurs. Notre PIB risque d'être fortement touché si nous épuisons notre tissu économique en ne lui donnant pas les moyens de payer une cyberrançon. Or le Sénat a fortement préconisé aux compagnies d'assurance de ne plus mettre en garantie de leurs contrats les paiements de cyberrançons.

Par ailleurs, l'Assemblée nationale et le Sénat travaillent déjà avec les assureurs et la FFA pour augmenter le niveau de prévention des entreprises,

mais elles ne sont pas tenues de souscrire aux contrats qui imposent un certain niveau de prévention.

### **M. Jérôme Notin**

La FFA est membre fondatrice de notre dispositif. Nous travaillons ensemble quotidiennement pour proposer des offres « cyber » qui répondent aux besoins des entreprises et assurent le risque résiduel.

En revanche, le paiement des rançons me choque énormément.

### **M. Michel Van Den Berghe**

Un des architectes qui travaille avec nous m'a consulté un matin, car il a été victime d'un *ransomware*. Son cabinet compte 80 professionnels qui travaillent sur Apple. Il a sollicité l'aide de nos experts alors qu'il ne pouvait plus accéder à aucune donnée, car ses sauvegardes étaient en ligne. Toutes les données étant encryptées, nous n'avons pas pu agir.

Il a finalement payé la rançon demandée (10 000 euros en bitcoins) pour récupérer l'ensemble de son système d'information, mais n'a rien réclamé à son assureur. J'estime que nous devons nous mettre à la place du dirigeant qui agit pour refaire fonctionner son entreprise.

Nous devons donc sensibiliser les chefs d'entreprise et leur proposer des moyens de résilience leur permettant, en cas d'attaque, de redémarrer leur entreprise sans payer la rançon.

### **M. Marc Bothorel**

Nous ne souhaitons pas que cette assurance devienne obligatoire pour les entreprises, mais nous conseillons fortement aux dirigeants de l'étudier pour protéger leur patrimoine.

Je participe également au groupe de travail du Trésor initié fin juin. À cette occasion, j'ai regardé les critères d'éligibilité que fixent les assurances. J'ai constaté un aspect mercantile dans les questionnaires très légers de certaines compagnies.

Les travaux que mène actuellement le Trésor, notamment sur un *rating* et des outils d'analyse et d'assurabilité, feront évoluer la situation. L'année dernière, les assurances ont payé deux fois plus de primes qu'elles n'en ont perçues. C'est aussi pourquoi le paiement des rançons a été retiré de certains contrats.

La prévention et la sensibilisation restent essentielles pour que l'entreprise soit assurable.

### **M. Emmanuel Cugny**

Ce vaste débat est à la fois technique et politique.



### **M. Patrick Bergougnou, Président du groupe Cirpack**

J'aimerais aborder un sujet de cybercriminalité « légale ». Le développement du télétravail et des formes de travail hybride génère l'utilisation d'outils de communication d'entreprise qui sont massivement déployés dans les entreprises (Microsoft Teams, Cisco Webex, Salesforce, Slack, Zoom ou encore Facebook, WhatsApp et Messenger).

Tous ces outils sont des plateformes américaines, soumises à l'*Internet Privacy Act* : l'administration américaine a donc accès à toutes les données de communication des entreprises sur simple demande réquisitoire.

Quelles dispositions le Sénat a-t-il prévu pour sensibiliser les entreprises sur ce sujet et mobiliser les moyens de soutenir les plateformes européennes et françaises ?

### **M. Marc Bothorel**

La CPME préconise aux dirigeants de se référer aux outils recommandés, testés et validés par l'ANSSI.

### **M. Sébastien Meurant, Sénateur du Val d'Oise**

Sénateur du Val-d'Oise, je suis aussi l'un des rapporteurs du rapport de notre Délégation aux entreprises sur ce sujet. Cette question touche la souveraineté et notre capacité, française et européenne, à avoir un *cloud* souverain sécurisé.

Cette question est majeure pour l'avenir de l'indépendance française et européenne. Certaines grandes entreprises françaises se sont rapprochées des entreprises du GAFAM, lesquelles assurent qu'elles ne dévoileront aucune donnée à la demande de l'administration américaine.

Cette question est cruciale pour l'avenir du pays : la reconquête de la souveraineté dépendra de la réussite des acteurs du Campus Cyber. En tant que rapporteur, pour la Délégation sénatoriale aux entreprises, j'ai constaté la naïveté de nombreuses entreprises et collectivités sur ce sujet. J'ai donc été enthousiasmé qu'une prise de conscience au plus haut niveau de l'État se traduise par la création de ce campus, car la reconquête de notre souveraineté est une des clés de l'avenir et de l'indépendance du pays.

### **M. Michel Van Den Berghe**

Les outils évoqués sont installés sur des systèmes d'exploitation, généralement fournis par Microsoft. Nous devrions donc utiliser un PC français équipé d'un OS français sur du matériel français ?....

Orange a beaucoup investi dans la création du *cloud* souverain 100 % français. Il n'a pas fonctionné. Nous essayons à nouveau en équipant les meilleures technologies d'outils permettant de détecter qu'aucune malversation, volontaire ou involontaire, n'est faite sur les données stockées.

Cette solution ne fonctionnera que si les entreprises acceptent de payer 20 à 30 % supplémentaires pour stocker leurs données sur un *cloud* souverain. La souveraineté a un coût que les entreprises ne souhaitent pas toujours supporter. Je rappelle également que les données extrêmement essentielles ne sont pas encore stockées dans le *cloud*.

Il n'est pas possible de placer l'ensemble des technologies utilisées sous une souveraineté globale, car 90 % de l'équipement numérique est fabriqué par les Américains.

### **M. Philippe Clerc**

Cette question permet de resituer la stratégie de lutte contre la cybercriminalité - donc la stratégie nationale de cybersécurité - au sein d'une politique publique de sécurité économique. À la direction générale des Entreprises, le Service de l'Information stratégique et de la Sécurité Économiques (SISSE) inclut cette vision stratégique essentielle.

Par ailleurs, l'Europe se mobilise sur le sujet de la souveraineté : notre secrétaire d'État chargé du Numérique a récemment réuni le *dataspace* français. La plateforme Gaïa X est un espace de données sécurisées qui réunit, dans le cadre européen et à l'échelle française, notre pôle de compétitivité, l'académie des Technologies, la Fédération des Industries Électriques, Électroniques et de Communication et les acteurs majeurs du numérique.

### **M. Stéphane Blanc, Président d'AntemetA, entreprise des Yvelines**

Je souhaite rappeler l'importance de l'assurance risque « cyber », notamment pour les ETI : comment peuvent-elles justifier auprès de leurs banquiers et actionnaires qu'elles ne sont pas assurées alors qu'elles ont réalisé les investissements nécessaires pour sécuriser leurs données ?

### **M. Christophe Delcamp, Représentant de la Fédération française des assurances (FFA), en charge des risques « cyber »**

Ma première réaction est de proposer d'organiser un débat sur l'assurance « cyber », car de nombreuses idées reçues méritent d'être confrontées à des réponses réalistes.

Depuis des années, la FFA souhaite accompagner les entreprises sur ce nouveau risque. Or, l'État doit disposer de toutes les informations pour pouvoir se positionner sur les rançons - les assureurs suivront cette position. Le rapport de la députée Mme Valéria Faure-Muntian, récemment publié, évoque ce sujet.

De plus, le risque « cyber » est nouveau et a une potentialité de risque systémique. Les assureurs doivent protéger tous les assurés sans s'exposer eux-mêmes au seul risque « cyber », qui doit être compris. L'ACPR, qui est

notre organisme de régulation, nous a demandé de travailler sur la protection de nos engagements.

Dans le cadre des travaux de la direction générale du Trésor qui aboutiront sur un rapport en février prochain, des pistes de solutions concertées sont susceptibles d'être envisagées pour fluidifier ce marché.

### **M. Sébastien Garnault, Fondateur de CyberTaskForce**

Le rapport de Mme Valéria Faure-Muntian publié la semaine dernière pourrait effectivement servir de support à un prochain débat du Parlement.

J'ajoute qu'un collaborateur qui n'a été ni sensibilisé, ni formé, ni outillé ne peut être considéré comme un « maillon faible ». La prise de conscience et l'engagement du dirigeant entraînent des conséquences sur l'assurance.

Je souhaite aborder le lien qui existe entre les collectivités et l'écosystème économique local : quelle différence voyez-vous entre une petite ville et une PME, notamment en matière de prise de conscience des dirigeants ? Existe-t-il des actions territoriales ?

### **M. Marc Bothorel**

Le fait que l'humain est un « maillon faible » est un simple constat. Nous souhaitons évidemment le rendre fort, car il constitue le premier rempart.

Le chef d'entreprise qui a pris conscience du risque doit inculquer une culture « cyber » à ses employés pour leur faire comprendre qu'ils font partie de la chaîne de défense de l'entreprise.

M. Jérôme Notin et moi-même avons participé au récent Forum international de la Cybersécurité. Une initiative très intéressante de la région des Hauts-de-France y a été présentée.

### **M. Jérôme Notin**

Lorsque nous aidons les entreprises, les collectivités ou les particuliers, nous commençons toujours par les qualifier. Nous aidons davantage de particuliers - 40 à 50 millions - que d'entreprises - trois à quatre millions - et de collectivités - 35 000, mais, compte tenu de la population éligible, pour un particulier aidé, nous aidons deux entreprises et quarante collectivités territoriales.

Ces dernières restent plus impactées que les entreprises, car elles subissent une certaine dette technique. Certaines collectivités n'ont pas encore conscience du risque « cyber ». C'est pourquoi nous avons priorisé le traitement des collectivités en 2019.

Nous avons annoncé au Forum international de la cybersécurité (FIC) le dispositif « Immunité Cyber » : ce questionnaire très pragmatique comportant neuf questions a été envoyé par l'AMF. Les collectivités ayant

répondu « non » au moins une fois sont invitées à prendre contact avec la gendarmerie afin d'être sensibilisées au risque de cybercriminalité.

Des actions sont donc menées dans les territoires, car les collectivités sont proportionnellement plus touchées par la cybermalveillance que les entreprises ou les particuliers.

#### **M. Rémi Cardon, Sénateur de la Somme**

Jeudi prochain, une table ronde sera organisée sur le sujet de la cybersécurité des collectivités, conjointement par la Délégation aux entreprises et la Délégation aux collectivités territoriales du Sénat.

Nous constatons en effet que les collectivités territoriales sont souvent touchées et que les maires connaissent une problématique de stockage des données. Pourtant, les collectivités, qui gèrent de l'argent public, doivent être exemplaires dans ce domaine.

#### **Mme Annick Billon, Sénatrice de Vendée, Présidente de la Délégation aux Droits des Femmes et à l'égalité des chances entre les hommes et les femmes du Sénat**

La culture du risque informatique demande un travail préalable important. Elle devra aussi être quotidienne pour s'adapter, car l'innovation sera multiforme dans ce secteur.

Lors d'un événement, j'ai eu l'occasion d'échanger des cartes de visite : un interlocuteur m'a invité à lui présenter mon téléphone afin que sa carte s'y inscrive directement. Ce type de situation présente-t-il un risque ?

Je vous remercie d'avoir évoqué les stéréotypes de genre qui agissent sur l'orientation, car nous travaillons avec la Délégation aux entreprises sur ce sujet.

#### **M. Jérôme Notin**

Vous avez certainement scanné un *QR Code* vous permettant de récupérer de informations encodées, car un *QR Code* permet soit de récupérer directement des informations, soit d'orienter vers un site web.

La sécurité du *QR Code* fait l'objet de débats dans notre communauté, car certains *QR Codes* permettent, *via* internet, de récupérer une charge malveillante.

#### **Mme Brigitte Devésa, Sénatrice des Bouches-du-Rhône**

Vous avez évoqué les moyens mis à la disposition des entreprises pour éviter les cyberattaques.

Aujourd'hui, comment une entreprise peut-elle accepter de payer une rançon ? Existe-t-il un service de police ou de gendarmerie spécialisé ?

Je suis choquée qu'une entreprise soit contrainte de céder au chantage des criminels pour continuer à travailler. Quels dispositifs permettent aux entreprises de se défendre et de récupérer ce qui leur a été volé ?

**M. Jérôme Notin**

Les services de l'État en police judiciaire sont bien organisés aujourd'hui, même s'ils méritent encore d'être renforcés. La police bénéficie de services d'enquête, d'un office central et d'un parquet spécialisé dont les trois magistrats ont été représentés lors d'une audition au Sénat récemment. Ils traitent les attaques de pays étrangers qui atteignent nos opérateurs d'importance vitale et nos structures régaliennes, mais aussi les crimes crapuleux qui extorquent des petites sommes à des milliers de victimes. Leur champ d'intervention est donc extrêmement large.

Le chef d'entreprise est responsable lorsqu'il décide de payer une rançon ; le remboursement de la rançon relève d'un débat politique, qui mérite d'avoir lieu et d'être enrichi de nouvelles tables rondes.

Enfin, l'intérêt fondamental de l'assurance « cyber » réside dans l'incitation à réaliser des sauvegardes déconnectées permettant de restaurer les données.

**M. Mickael Mesere, Marketing Digital Manager**

Existe-t-il des services qui permettent de réaliser un diagnostic de la santé informatique d'une entreprise ?

**M. Marc Bothorel**

Vous avez découvert *cyberveilleance.gouv.fr* et son nouveau volet d'activité, la sécurisation des entreprises au travers du réseau d'entreprises labellisées « ExpertCyber » mis en place depuis début 2021 - mon entreprise est ainsi labellisée.

L'initiative de France Services concernant les conseillers numériques est extrêmement intéressante et importante. Pour autant, il est regrettable que le volet « cyber » de leur formation soit quasi inexistant.

**M. Jérôme Notin**

50 petites entreprises sont effectivement labellisées « ExpertCyber » dans les territoires. Comme les prestataires de l'ANSSI, elles ont la capacité de réaliser de la remédiation et d'accompagner les entreprises dans leur démarche de sécurisation (hébergement, infrastructures), mais proposent des tarifs nettement plus bas.

L'AFNOR s'appuie sur un référentiel, sur lequel nous avons travaillé notamment avec la FFA et la CPME, pour s'assurer du niveau d'expertise des « ExpertCyber ». Ces prestataires de proximité pourront adresser l'ensemble des besoins sur l'ensemble des territoires.

### **M. Philippe Clerc**

Ces réponses illustrent parfaitement l'évolution du parcours de sécurisation des chefs d'entreprise en matière de cybersécurité. Les chambres de commerce ont l'obligation de progresser au sein de cette chaîne d'intervention. Aujourd'hui, 18 chambres sont agréées par France Compétences sur la base d'un référentiel mis en place par l'ANSSI.

Cet écosystème se développe et une chaîne d'intervention se met en place afin de diagnostiquer le risque et d'orienter l'entreprise en fonction du degré de criticité de sa situation.

### **Un intervenant**

Je suis chef d'entreprise et auditeur en cybersécurité à l'Institut des hautes études de défense nationale (IHEDN). La coopération entre les États membres sera-t-elle encouragée afin de lutter contre les cybercriminels, dont 60 % se trouvent à l'étranger ?

### **M. Andreas Koch, Gérant et co-fondateur de Cortex Productions, membre associé de la CCI de Charente**

Je souhaite souligner que la problématique de la rançon est d'abord morale, car elle place le chef d'entreprise dans une situation extrêmement délicate.

Les comportements criminels doivent sortir de l'anonymat afin que naissent des lois et des organisations nécessaires pour les combattre.

### **M. Christophe Langlès, co-président de la CPME 13**

Pourquoi sommes-nous défavorables à l'intégration obligatoire du contrat d'assurance dans les contrats responsabilité civile (RC) d'entreprise ? Je rappelle qu'un contrat cybercriminalité prévoit la mise à disposition d'une plateforme de conseillers, l'indemnisation de l'intervention des informaticiens et la réponse à la mise en cause de la responsabilité civile professionnelle lorsque les données sont volées et susceptibles d'être exploitées.

### **M. Marc Bothorel**

La CPME recommande fortement cette intégration, mais ne souhaite pas l'imposer dans la période de reprise actuelle. Le chef d'entreprise reste responsable.

L'ensemble des syndicats patronaux a soumis une réponse commune à la nouvelle directive européenne *Network Information System* (NIS) qui impose aux petites entreprises (moins de 50 salariés et deux millions de chiffre d'affaires) des secteurs sensibles de respecter un certain niveau de cybersécurité. Nous souhaitons garder une décision de souveraineté en France sur ces sujets.

**M. Emmanuel Cugny**

Je vous remercie infiniment, chers intervenants.

*La séance est suspendue de 11 heures 13 à 11 heures 16.*





### III. THÈME 2 : PRÉVENTION EN SANTÉ ET BIEN-ÊTRE AU TRAVAIL

#### M. Emmanuel Cugny

Nous nous retrouvons pour la seconde partie de cette matinée de travail. Après l'urgence de la maîtrise de la cybersécurité, nous abordons une autre urgence à gérer dans le monde post-pandémie : la prévention en santé et le bien-être au travail.

Un nouveau paradigme apparaît en effet avec la crise sanitaire. Quels outils s'approprient pour un nouveau monde du travail ? Quels sont les bons interlocuteurs ?

Pour introduire cette table ronde, je vous propose d'écouter Madame Pascale Gruny, Vice-Présidente du Sénat et co-rapporteur de la commission des affaires sociales sur la loi du 2 août 2021 pour renforcer la prévention en santé au travail.

#### A. PRÉSENTATION DES ÉVOLUTIONS INTRODUITES PAR LA LOI « SANTÉ AU TRAVAIL »

*[Vidéo introductive]*

#### Mme Pascale Gruny, Vice-Présidente du Sénat

Bonjour à tous, je regrette de ne pas pouvoir être avec vous. En tant que rapporteur sur la loi pour renforcer la prévention en santé au travail avec M. Stéphane Artano, il me semble important que la Délégation aux entreprises se saisisse du sujet.

La première question que l'on peut se poser est celle de l'importance de cette loi pour les plus petites entreprises. Les partenaires sociaux ont réussi à s'entendre, dans le cadre d'un accord national interprofessionnel, sur ce texte particulièrement axé sur la prévention en santé et la sécurité au travail. Or, les PME peinent à s'approprier ce thème pourtant essentiel, car elles ne disposent ni du temps ni des structures internes nécessaires.

La démarche de prévention s'appuie sur le Document Unique d'Évaluation des Risques Professionnels (DUERP). Or, d'après les dernières statistiques disponibles, 50 % des entreprises n'avaient pas encore réalisé ce document, qui est pourtant la colonne vertébrale de la prévention en entreprise.

La prévention en entreprise consiste d'abord à protéger le dirigeant, car il doit respecter les obligations légales qui s'imposent en matière de santé, de sécurité et d'hygiène des salariés. Lorsque la direction d'une entreprise se préoccupe de ces thèmes, les salariés vivent beaucoup mieux.

Elle vise également à promouvoir la qualité de vie au travail. Actuellement, l'épuisement ou les difficultés professionnels sont souvent

évoqués. Ces sujets sont difficiles à appréhender pour des non-psychologues, alors qu'ils représentent une préoccupation très importante.

La prévention est essentielle pour la santé de l'entreprise.

La loi évolue légèrement pour ce qui concerne le document unique, notamment pour les entreprises de plus de 50 salariés. Un programme annuel de prévention des risques et d'amélioration des conditions de travail s'ajoute au DUERP. Ce programme fixe la liste détaillée des actions qui doivent être engagées pour prévenir les risques identifiés ainsi que leur coût et leur délai d'exécution.

Au Sénat, nous n'avons pas souhaité rendre ce plan obligatoire pour l'ensemble des entreprises, notamment pour ne pas alourdir les formalités administratives des plus petites entreprises. Au demeurant, ces dernières utilisent peu leur DUERP alors que ce document a vocation à évoluer régulièrement en fonction des éventuels accidents rencontrés. Il leur est donc simplement demandé de compléter leur DUERP avec les actions qu'elles envisagent de mettre en place pour prévenir les risques identifiés. Ainsi, le plan d'action ne fait pas l'objet d'un document supplémentaire.

Le DUERP doit être conservé pendant 40 ans. L'archivage de ce document a suscité de nombreuses interrogations. Nous avons décidé de mettre en place un portail numérique que les partenaires sociaux proposeront. La traçabilité des accidents et des expositions sera ainsi garantie.

Nous avons également souhaité harmoniser les services de prévention et santé au travail sur les différents territoires. Nous avons donc travaillé sur l'offre socle qui doit garantir le suivi des travailleurs, la prévention des risques professionnels et la prévention de la désinsertion professionnelle. Chaque service de prévention et santé au travail sera certifié et des services supplémentaires payants pourront être proposés en fonction des besoins de l'entreprise.

La santé des chefs d'entreprise a fait l'objet de toute notre attention, car elle conditionne la santé de l'entreprise et le maintien des emplois. Sans aller jusqu'à l'obligation – que je souhaitais à titre personnel, nous avons décidé de donner à tous les dirigeants la possibilité de rencontrer la médecine du travail. J'espère sincèrement qu'ils saisiront cette opportunité et se préoccupent de leur santé y compris dans sa dimension psychologique. Le chef d'entreprise doit quotidiennement répondre à de nombreuses exigences et affronter des difficultés, en étant souvent seul. La crise sanitaire a accentué ce phénomène.

Enfin, nous avons proposé une fourchette de prix afin d'éviter les écarts trop importants d'un service à un autre. La cotisation doit être la même pour une personne qui travaille à temps partiel.

Stéphane Artano et moi-même restons à votre disposition pour répondre aux questions que relaiera la DDélégation aux entreprises.

**B. TABLE RONDE : « QUELS OUTILS POUR UN NOUVEAU MONDE DU TRAVAIL ? »**

**M. Emmanuel Cugny**

Notre droit du travail est-il capable de répondre aux enjeux du nouveau monde ? Nous entrons effectivement avec un nouveau paradigme dans une nouvelle société économique et sociale.

**M. Jean-Emmanuel Ray, Professeur de droit à l'Université Panthéon-Sorbonne, spécialiste en droit du travail**

Je vous propose un plan en deux parties autour de la thématique de la santé mentale et de la santé numérique.

La santé mentale aujourd'hui

Je plaide coupable : les plus anciens d'entre nous ont vu paraître au JO en 2002 une loi actant le passage de la santé physique à la santé mentale. Je crains de ne pas avoir été le seul à ne pas voir la révolution entraînée par ce changement d'adjectif.

La santé physique demeure : les chutes de hauteur ne sont pas remises en question. La société du numérique concerne cinq millions de personnes sur 20 millions de travailleurs ; de nombreux salariés continuent d'assembler des pièces dans l'industrie et ne sont pas concernés par le télétravail.

Le changement qui s'est opéré est radical. En un siècle, le droit du travail avait fait le tour des règles relatives aux chutes de hauteur, aux gants de sécurité ou aux casques de BTP. Les accidents du travail sont aujourd'hui quatre fois moins nombreux qu'il y a 50 ans. De ce point de vue, le droit du travail a montré son efficacité.

Le concept de santé mentale a ensuite été introduit. Or, « l'homme n'est pas une île ». Le chef d'entreprise est responsable, car il tient la surveillance.

Un travailleur du savoir évolue dans les avions et les aéroports. Il rentre tard chez lui. Comment le chef d'entreprise peut-il suivre sa santé mentale, dès lors qu'elle concerne toutes les dimensions de sa personne - professionnelle et personnelle ? Comment distinguer le père de trois enfants en bas âge du travailleur qui arrive au travail sans avoir dormi de la nuit ?

Je crois que le changement nous a échappé : nous avons les moyens de contrôler la santé physique ; avons-nous les moyens de contrôler la santé mentale d'une personne unique ?

La théorie de Taylor évaluait la charge de travail à travers sa pénibilité et sa charge pondérale (durée ou produit de la durée et du poids). Cette mesure était simple et objectivable.

La charge pondérale d'un travailleur du savoir est accessoire. Quelle est la charge de travail d'un travailleur du savoir ? Quand travaille-t-il ?

Lorsque j'évoque le droit à la déconnexion avec mes étudiants, ils me demandent respectueusement de répéter et de préciser : « de quoi ? De qui ? ». Il existe un immense décalage de vision entre les générations. En effet, les jeunes ont toute leur vie dans leur téléphone. La déconnexion les réduirait à la mort sociale.

Certains juristes du travail préfèrent éviter cette question de peur de ne pas savoir la résoudre. Or le rôle d'un juriste est de trouver une solution pour ne pas créer de nids de contentieux.

La charge de travail est-elle évaluable ? Contrôlable ? Mesurable ? Nous ne savons plus mesurer la charge de travail, car elle est devenue informationnelle, communicationnelle et relationnelle.

La santé numérique aujourd'hui

La plupart des salariés français ne sont pas des cadres au forfait jours, mais réalisent un travail physique en entreprise. Le slogan « Singer libère le ménagère » n'est plus vérifié. Contrairement aux idées reçues, les nouvelles technologies ne libèrent pas le travailleur : elles ont un effet polarisant. Elles autorisent des marges de manœuvre seulement à quelques-uns.

La société du numérique introduit des problèmes radicalement nouveaux pour cinq millions de personnes. Le droit du travail ancien conserve donc toute sa place, car la subordination s'amplifie.

Finalement, le changement réside dans le don d'ubiquité : la loi de la pesanteur empêchait physiquement toute exportation du travail en dehors de l'entreprise alors que les données ont le don d'ubiquité. Or notre droit du travail est fondé sur le modèle industriel caractérisé par une unité de temps, de lieu et d'action.

Le chef d'entreprise assure la sécurité et la santé de ses collaborateurs. Mais comment peut-il garantir que le télétravailleur respecte les règles de sécurité ? La loi ne fait pas la distinction entre le domicile et le lieu de travail alors que les conditions d'exercice du travail diffèrent absolument (affichage de panneaux de secours, revêtement du sol des toilettes...).

Dans les années 1930, les usines croissaient tandis que le sort des travailleurs déclinait. Les syndicalistes, les employeurs et les universitaires ont eu à construire un droit du travail équilibré et protecteur du salarié. Désormais, l'enjeu réside dans la création d'un droit du travail adapté au travail à distance. C'est la raison pour laquelle je rappelle à mes étudiants, vos enfants, qu'ils auront à accomplir cette formidable tâche.

## **M. Emmanuel Cugny**

Un certain nombre de risques ont été mis en évidence par l'enquête qu'a menée l'ANACT pendant les différents confinements. Pourriez-vous nous expliquer ce qu'il en est ?

## **M. Matthieu Pavageau, Directeur technique et scientifique de l'Agence Nationale pour l'Amélioration des Conditions de Travail (ANACT)**

L'ANACT est reliée à un réseau d'Agences Régionales pour l'Amélioration des Conditions de Travail (ARACT). Nous sommes quotidiennement en relation avec les entreprises, car nous accompagnons un grand nombre d'entre elles, quel que soit leur secteur d'activité (privé ou public).

Plus de 2 000 répondants, issus de secteurs et de types d'entreprise différents, ont ainsi participé à la consultation que vous venez de mentionner. Nous disposons de nombreux travaux relatifs à la montée en puissance du travail à distance et à ses répercussions sur les situations de travail. Mais il existe également une série de travaux sur les 75 % des entreprises qui ont été moins concernées par les questions du travail à distance que par les problématiques de continuité du travail dans une période de crise ou de reprise après une période d'arrêt. En effet, l'accompagnement des grosses turbulences d'activité, l'efficacité, la productivité, la montée en charge avec des ressources limitées ou encore l'attractivité et le recrutement sont aussi des sujets de préoccupation des entreprises sur lesquels nous travaillons.

Vous avez introduit le nouveau monde et ses enjeux. Concernant les outils, certains chefs d'entreprise ont peut-être sollicité le dispositif national « Objectif reprise » et sa déclinaison « Objectif télétravail ». Ces dispositifs, dont certaines déclinaisons restent mobilisables, ont été mis en place par le ministère du Travail, l'ANACT et les ARACT pour accompagner très concrètement les petites entreprises qui font face à des questions d'une grande complexité. Notre action concerne trois sujets principaux :

- L'organisation du travail. Ce sujet est mis au premier plan aujourd'hui.
- Les relations professionnelles et sociales. Comment le manager doit-il agir lorsque l'activité est rompue ? Comment peut-il concilier le travail sur site des uns avec le travail à distance des autres ? Comment peut-il prendre en compte les inégalités de traitement perçues dans certaines équipes de travail, lorsque les tâches de certains leur permettent de travailler à distance tandis que les tâches des autres leur imposent d'être présents dans l'entreprise ? Les relations professionnelles et les relations sociales sont décisives.
- La santé. Les problématiques de santé mentale ont été particulièrement mises en évidence dans la période récente.

La consultation à laquelle vous faisiez référence concerne les emplois télétravaillables, qui représentent un quart à un tiers des emplois. Selon les statistiques de la DARES, le télétravail représentait seulement 3 % en 2017. Les salariés concernés travaillaient à distance au moins un jour par semaine. La crise a engendré une forte augmentation du télétravail - jusqu'à 35 % dans certaines périodes, même si le phénomène a oscillé en fonction du besoin de travailler sur site et de l'importance de la relation de travail.

Nous avons connu une situation de télétravail exceptionnelle dont nous pouvons tirer de précieux enseignements, mais qui ne peut pas faire référence pour construire l'avenir. Nous devons encore construire un modèle de référence. Les entreprises ont encore besoin de tester plusieurs modalités d'organisation et de contrôle du travail à distance.

En fonction des secteurs d'activité, les cultures d'entreprise et les pratiques restent très différentes. Dans ce contexte, l'ANACT n'envisage pas d'imposer une organisation de travail, mais elle mettra en évidence des points de vigilance. Certains ont été identifiés lors de la consultation, car elle a permis de partager les expériences vécues. Les tendances majeures s'avèrent très intéressantes pour l'avenir de l'humain au travail :

- On se sent à la fois plus efficace et plus fatigué lorsque travail est réalisé à distance.
- En 2021, si 90 % d'entre nous souhaitent continuer à travailler à distance, un tiers seulement pourra travailler trois jours par semaine ou plus.

Deux enseignements sont donc à souligner. Tout d'abord, la fatigue et l'investissement mettent en évidence une forme de dérégulation incontournable que le *management* peine à appréhender en raison de sa moindre maîtrise de la situation. Ensuite, les relations au travail (lien avec les collègues et le manager, conséquences de la distance) ont des effets sur la santé mentale, laquelle repose sur l'identification et la reconnaissance de l'individu au travail et ses projections pour l'avenir. Or, certains facteurs y nuisent terriblement.

### **M. Emmanuel Cugny**

Le télétravail s'est imposé pendant la pandémie et a profondément modifié notre rapport aux tâches quotidiennes. Il y a quelques années, l'Organisation Internationale du Travail (OIT) a publié un rapport identifiant trois principaux enjeux du travail dans la société : la mondialisation, l'automatisation et la robotisation. Madame Breton Kueny, vous y avez apporté des éclairages supplémentaires à l'aune de cette actualité. Nous vous écoutons.

**Madame Laurence Breton Kueny, Vice-Présidente de l'Association Nationale des Directeurs des Ressources Humaines (ANDRH), Présidente de la commission Santé au travail, DRH du groupe AFNOR**

J'aimerais revenir sur ces nouveaux enjeux du dialogue social en faisant référence à ce rapport de l'OIT qui date de 2017. Aujourd'hui, nous devons travailler au niveau local mais penser au niveau international, car nous prendrions des risques en n'agissant pas ainsi. Ces enjeux sont effectivement liés au thème du télétravail sur lequel vous m'interrogez :

- La mondialisation et la financiarisation de l'activité économique, premier enjeu du dialogue social :

Nous avons constaté que le télétravail et la numérisation mettent en concurrence les salariés à travers le monde. Or, dans certains pays, le coût du travail et la protection sociale sont moindres. Il convient donc de distinguer le lieu où se déroule la négociation de celui où se réalise l'activité.

- L'automatisation et la robotisation dans l'industrie :

Ce phénomène est connu depuis longtemps et a vocation à s'accélérer. La numérisation et la digitalisation seront également utilisées dans le traitement de l'information. Il sera désormais possible d'utiliser des algorithmes, les *Robotic Process Automation* (RPA), pour remplacer une partie de l'activité des salariés.

C'est pourquoi, en tant que DRH, nous estimons important de participer aux négociations pour préparer la gestion des emplois et des parcours professionnels - en France - et le *Strategic Workforce Planning* - à l'international. À titre personnel je préfère cette dernière approche car aujourd'hui, nous ne pouvons pas nous contenter de travailler sur le champ des salariés. Nous devons envisager l'ensemble de la main-d'œuvre et toutes ses formes. À titre d'exemple, vous savez qu'en entreprise, les notes de frais Uber sont remboursées. Or, la société Uber ne garantit pas la même couverture sociale qu'une société de taxis traditionnelle. Nous ne devons pas oublier les travailleurs de la *Gig Economy*, car ils se multiplieront.

- La transition écologique :

Les nouvelles générations se préoccupent de la question de la dégradation et des sujets d'économie circulaire. Je rappelle d'ailleurs que la France détient la présidence de la commission internationale de Normalisation sur l'économie circulaire, qui est le sujet d'avenir. J'en profite pour signaler, pour ma propre profession, qu'il n'y a à aucun directeur des ressources humaines, ni au niveau français ni au niveau international, alors que cela aura un impact sur les compétences.

Je souhaite ajouter deux enjeux à ceux qu'a identifiés l'OIT :

- La transition démographique :

Notre pays vieillit : depuis 1950, nous avons gagné seize ans d'espérance de vie. Cette évolution soulève la problématique des retraites (1,7 actif pour un inactif) et celle de l'allongement de la durée d'activité que doivent gérer les DRH.

Le dernier baromètre Odoxa a montré que deux tiers des personnes qui entrent en retraite ne sont déjà plus en activité. Au niveau international, nous travaillons sur l'*Aging Society* et l'*Aging Workforce* : en France, l'âge de mise à la retraite d'office est récemment passé de 65 à 70 ans et la Grande-Bretagne n'impose plus d'âge de mise à la retraite depuis quelques années. Mes homologues me disent régulièrement que les personnes ne meurent pas du travail, elles meurent au travail.

- La santé :

J'utilise toujours la définition de l'OMS : « La santé est un état complet de bien-être physique, mental et social et ne consiste pas seulement en une absence de maladie ou d'infirmité. »

Or, en période de télétravail, la question sociale a manqué. La récente enquête menée par l'ANDRH a montré l'influence grandissante des aspects individualistes dans les évolutions d'organisation et l'importance des risques psychosociaux.

Enfin, je souhaite souligner l'importance des propos de M. Jean-Emmanuel Ray concernant nos demandes d'évolution du Code du travail et la problématique que nous rencontrons dans les accords que nous signons. Aujourd'hui, si 50% d'entre nous pouvons nous appuyer sur des accords, ces derniers sont mis en cause par 15 % des salariés en raison de l'éligibilité des métiers, du nombre de jours travaillés et du montant des indemnités.

Plus les salariés s'éloignent de l'entreprise et plus ils formulent des demandes individuelles, comme la prise en charge de la moitié des frais de déplacement suite à un déménagement ou la semaine de trois jours (du mardi au jeudi). Nous estimons que nous ne devons pas nous faire imposer les choix de vie personnels, car l'écosystème entier risque d'être impacté par la montée des individualismes. Une entreprise implantée fait vivre tout un bassin économique (services de ménage, de restauration, de sécurité).

Par ailleurs, nous devons veiller à l'équité de traitement - le télétravail ne concerne que quelques salariés - ainsi qu'au mode de vie des personnes. Cette crise a révélé des inégalités sociales : certaines personnes vivent dans des conditions qui ne leur permettent pas de travailler à distance (logement exigü, famille nombreuse). C'est pourquoi dans mon groupe nous avons réouvert le 18 mai 2020 et n'avons jamais refermé. L'entreprise reste un rempart de protection qui ne peut pas être sacrifié au titre des avantages



individuels. L'entreprise doit trouver une protection pour l'ensemble des salariés.

Enfin, nous ne sommes pas favorables au télétravail à 100 %, car il ouvre la porte aux délocalisations de demain.

### **M. Emmanuel Cugny**

Quelles sont les attentes des salariés et comment vivent-ils dans l'entreprise après l'accord national interprofessionnel (ANI)?

### **Mme Bénédicte Moutin, Secrétaire confédérale de la CFDT, en charge du volet « vie au travail-dialogue social ».**

L'ensemble des développements précédents fait écho aux attentes des représentants du personnel et des salariés.

Le Code du travail, le nouvel ANI et la loi constituent le cadre légal ou réglementaire. Or, la prévention relève du droit, mais aussi des pratiques et des cultures d'entreprise. Dès lors, comment encourager la prévention à l'avenir ? Ces textes ambitieux constituent des supports indéniables, qu'il convient néanmoins de dépasser pour aborder efficacement le changement de paradigme. Certains éléments du nouvel ANI sur la santé au travail ont été facilement transposés dans la loi tandis qu'un socle de droit mou ne l'a pas été en raison de sa complexité. Aucune assise normative extrêmement puissante ne concerne ce droit mou.

Les employeurs restent attachés au droit. Ils recherchent une sécurité juridique, notamment au sujet des questions de santé au travail et de protection des salariés. Dès lors, comment faire de la sécurisation juridique un objet de dialogue social et professionnel permettant d'encourager la culture et les pratiques de prévention ? Ces questions doivent être abordées en amont pour traiter des conditions de travail.

Ces deux textes doivent donc être complétés d'éléments de culture de prévention pour garantir la prévention, notamment primaire. Un employeur peut tout à fait légalement décider de changer une machine et son implantation, sans évaluer au préalable les risques professionnels liés à son installation. Il lui suffira d'enrichir le DUERP *a posteriori* pour respecter ses obligations légales. Pourtant, la consultation préalable des représentants du personnel et des travailleurs concernés sur l'objectif et l'impact du remplacement de matériel facilite la conduite du changement et limite les risques professionnels en amont.

Nous estimons que le dialogue social et professionnel doit être envisagé comme un complément du cadre légal pour faire avancer les questions de prévention.

Nous avons constaté la difficulté de mobiliser les branches professionnelles sur ce sujet et d'ancrer des avancées dans le cadre légal. Contrairement à d'autres pays européens, le système de santé au travail en

France s'appuie davantage sur le principe de réparation que sur le principe de prévention. Or, les mesures de réparation ne remplacent jamais la santé du salarié ni ses compétences dans l'entreprise.

La CFDT estime que le travail doit construire la santé des salariés. Tous les dispositifs et toutes les énergies doivent donc être mobilisés pour concourir à la prévention de la santé des salariés dans une approche élargie du travail, c'est-à-dire pas uniquement centrée sur les risques professionnels.

Nous avons négocié l'ANI et nous sommes satisfaits que la loi transpose des éléments concernant l'accompagnement des entreprises, la prise en compte de la Qualité de Vie au Travail (QVT) et l'évolution des services de santé au travail et du DUERP.

En 2016, la CFDT a réalisé une grande enquête sur le travail, à laquelle 200 000 travailleurs, adhérents ou non à la CFDT, ont répondu. 44 % d'entre eux souhaitent que leurs représentants du personnel agissent pour améliorer les conditions de travail. 14 % ont cité la défense de l'emploi ; 10 %, les conseils sur la situation de travail ; 9 %, le maintien du pouvoir d'achat ; 9 %, l'égalité hommes-femmes et 5 %, le maintien du système de retraite. La notion de conditions de travail apparaît donc comme centrale. La crise sanitaire l'a d'ailleurs mise en évidence à travers l'exercice du télétravail, les mesures de protection et la non-préparation des entreprises. Le développement de l'anticipation et de la culture de prévention est donc nécessaire pour progresser collectivement.

### **C. DÉBAT**

#### **M. Emmanuel Cugny**

Professeur Ray, vous nous avez dressé un portrait disruptif du droit du travail. Pouvons-nous véritablement parler d'« ubérisation » du droit du travail aujourd'hui ?

#### **M. Jean-Emmanuel Ray**

Cette question est essentielle et je dirais que lorsque le droit encourage l'hypocrisie, il n'est pas adapté et il faut le changer. Je vous donne un exemple très concret : aujourd'hui, pour de nombreuses raisons, le travail à domicile encourage l'hyperconnexion. Un juriste consulté sur les risques engendrés par cette situation de travail interrogera le chef d'entreprise sur le nombre de travailleurs concernés et leur temps de travail. Or ce dernier ignore souvent le temps de travail effectué par ses télétravailleurs, car il est satisfait de la situation : le travail est accompli et le télétravailleur est content.

Mais la chambre sociale de la Cour de cassation a rendu un arrêt le 8 juillet 2020. Le demandeur, un *webmaster*, travaille entièrement à son domicile, à Grenoble. Ses horaires atypiques lui conviennent parfaitement et

son travail efficace satisfait son employeur. Lorsque son employeur le licencie, ce *webmaster* saisit le conseil des prud'hommes de Grenoble en réclamant 271 000 euros de dommages et intérêts, cette somme correspondant à la rémunération des heures supplémentaires, du travail dominical et du travail de nuit.

La cour de Grenoble a demandé au salarié de prouver qu'il a travaillé 60 heures par semaine pendant trois ans - ce volume horaire correspond à douze heures de travail quotidien en continu. Autrement dit, la Cour a sollicité du demandeur qu'il présente, pour chaque journée travaillée, ses horaires de connexion et de déconnexion.

Nous assistons aujourd'hui à un télescopage insupportable entre le droit de la durée du travail et le télétravail au domicile. Le recours en cassation est assuré s'il est demandé au salarié d'apporter ses preuves. En effet, le Code du travail stipule qu'en cas de contestation sur les heures supplémentaires, il appartient à l'employeur de démontrer que les heures de travail ont été réalisées et que les temps de repos ont été respectés - je précise que le temps de repos, onze heures minimum, concerne aussi les salariés au forfait jours.

Dans ce type de litige, la Cour de cassation rappellera systématiquement que la charge de la preuve pèse sur l'employeur. Or, l'employeur n'a pas la capacité de démontrer que le salarié n'a pas travaillé alors qu'il était connecté. Il sera donc systématiquement débouté : ça ne tourne pas rond.

### **M. Emmanuel Cugny**

Actuellement, les chefs d'entreprise appréhendent-ils le droit du travail comme une aide ou, au contraire, le craignent-ils ?

### **M. Jean-Emmanuel Ray**

Je ne voudrais pas vous effrayer mais un salarié qui souhaite négocier une rupture conventionnelle est en position de force. En effet, l'employeur qui n'a pas déclaré les heures de travail réalisées commet un délit correctionnel de travail dissimulé.

Je disais que ça ne tourne pas rond car ce contexte réglementaire encourage l'hypocrisie : un DRH qui souhaite éviter la chambre correctionnelle peut ordonner à son service informatique de couper les serveurs à 19 heures 30. Ainsi, l'amplitude journalière officielle ne dépassera pas treize heures (24 heures moins onze heures de repos), mais les salariés seront implicitement invités à enregistrer leurs documents sur une clé USB pour poursuivre leur travail.

Le droit ne doit pas encourager l'hypocrisie. Ses normes sont issues du milieu industriel : la pointeuse reste utile, mais des adaptations sont nécessaires.

La directive européenne de 2003 impose au salarié de pointer ses heures de travail sauf lorsqu'il est autonome. J'estime donc nécessaire de faire évoluer le droit communautaire en assimilant à des cadres autonomes les personnes en situation de télétravail.

Si les chefs d'entreprise, qui ne peuvent pas surveiller leurs salariés lorsqu'ils travaillent à leur domicile, ne sont pas vigilants, ils risquent le tribunal correctionnel. Ils seront donc *in fine* encouragés à externaliser les services télétravaillables.

### **M. Emmanuel Cugny**

Merci Professeur pour cette démonstration. L'apprentissage est souvent évoqué pour lutter contre le chômage de masse. Comment gérer les questions d'apprentissage avec le télétravail ? Ce sujet fait-il l'objet d'une réflexion aujourd'hui ? Nous assistons à une rupture, car l'apprentissage repose sur un contact humain.

### **M. Matthieu Pavageau**

Nous estimons qu'il ne peut y avoir d'apprentissage sans confrontation à la situation de travail - les formations qui n'offrent pas cette possibilité sont souvent décalées par rapport aux besoins réels. La mise à distance est donc susceptible de compliquer la mise en œuvre de ce type de dispositif.

Plus généralement, la question de la compétence doit être liée aux enjeux du recrutement dans certains secteurs d'activité et de l'attractivité des métiers en tension : d'une part, la mise à distance complique la formation en situation de travail ; d'autre part, certains secteurs rencontrent de grandes difficultés pour attirer et fidéliser les compétences.

Nous développons un programme à destination de certains secteurs pour activer le levier de l'amélioration des conditions de réalisation du travail, car la plupart des secteurs exposés aujourd'hui sont relativement sinistrés en matière de conditions de travail.

Nous estimons qu'il faut soutenir les secteurs qui rencontrent des difficultés de recrutement. La question essentielle concerne les conditions de réalisation du travail. Dans ce contexte, il convient de donner la possibilité aux ressources potentielles de se projeter dans un secteur qui offre des garanties en matière de sécurité des emplois.

Concernant l'apprentissage, nous estimons qu'une formation n'est efficace que si elle prévoit des situations de travail. Elle aboutit alors à l'intégration réussie et à la fidélisation. Par ailleurs, les entreprises ont sûrement besoin d'apprendre à faire face collectivement à des moments de turbulence.

### **M. Emmanuel Cugny**

Le dialogue social reste indispensable dans ce contexte.

### **Mme Bénédicte Moutin**

L'entreprise doit articuler le dialogue social et le dialogue professionnel : le dialogue social est organisé par la loi, qui a renforcé le rôle du CSE et appuyé le rôle de la négociation ; le dialogue professionnel se construit avec les travailleurs et concerne les conditions de réalisation du travail. Tous les acteurs de l'entreprise (l'employeur, les représentants du personnel et les travailleurs) doivent participer à cette dynamique collective.

### **Mme Laurence Breton-Kueny**

En France, nous avons la chance d'avoir un système de santé efficace. Je souhaiterais évoquer la norme québécoise « Promotion, prévention de la santé en entreprise », qui date de 2008 et qui est devenue canadienne en 2020, englobe quatre dimensions :

- Les saines habitudes de vie : 50 % des pathologies que nous développons s'expliquent par le mode de vie. Les entreprises deviennent les premiers préventeurs.
- **Les pratiques de management**, qui jouent un rôle central dans les risques de santé mentale.
- L'environnement de travail, qui inclut les transports et les modes de garde.
- L'équilibre vie privée-vie professionnelle, très important dans le cadre du télétravail.

Les travaux que le professeur universitaire québécois Alain Marchand a réalisés il y a une dizaine d'années évoquent les facteurs de protection et de risque par rapport à la déprime, la dépression et l'épuisement. Or les DRH observent que l'épuisement est souvent mixte - il est à la fois personnel et professionnel. C'est pourquoi nous estimons que le *burn-out* ne doit pas être systématiquement reconnu comme une maladie professionnelle, mais démontré dans chaque cas.

Le dernier baromètre « Empreinte Humaine » montre qu'actuellement plus de 30 % des personnes ne se sentent pas bien. En région parisienne, une majorité de salariés vivent seuls et l'entreprise devient le premier lieu de lien social. Dans ce contexte, la responsabilité de l'employeur doit être délimitée, car il doit déjà gérer la question économique et de l'emploi.

### **Un intervenant**

J'ai créé une PME d'environ 100 personnes il y a 30 ans et je suis également maire d'une commune de 2 200 habitants. Nous avons évoqué la médecine du travail, qui est censée suivre les employés et s'assurer de leur bonne santé.

Quand j'ai commencé mon activité dans les années 1990, l'employeur payait une visite par an. Les visites, pourtant toujours payées chaque année,

se sont ensuite espacées tous les deux ans et depuis la loi Travail de 2016, tous les cinq ans. Pourtant les entreprises continuent à payer 3,28 % de leur masse salariale avec un plancher de 70 euros par salarié et par an. Ainsi, la visite revient à 350 euros tous les cinq ans.

J'estime cette évolution anormale, car l'entreprise paye toujours davantage alors que le service s'éloigne du salarié. L'un de mes salariés a appris qu'il souffrait d'un cancer de la prostate grâce à la visite médicale. Celle-ci est essentielle et pourtant les salariés sont de moins en moins suivis.

Enfin la santé des chefs d'entreprise a été évoquée : pour la conserver, il serait judicieux de moins les taxer.

### **Mme Laurence Breton-Kueny**

J'approuve totalement vos propos. Pourtant, j'ai la chance d'avoir un service médical en interne avec une infirmière salariée et notre médecin du travail acceptera de revenir après son départ en retraite, car il fait partie des nouveaux services de prévention et de santé au travail.

Nous souffrons aujourd'hui d'un déficit en compétences de médecins du travail. Des infirmières peuvent réaliser des entretiens infirmiers, mais la gestion des retours après une absence de longue durée reste compliquée. Dans mon entreprise, nous sommes régulièrement obligés de demander aux personnes de rester chez elles en attendant qu'une visite soit programmée, alors que nous sommes assez chanceux en Ile-de-France. Dans certaines régions on ne trouve pas de médecins du travail. Tous les départs à la retraite ne sont pas remplacés. Dès lors, la question de la formation et de la reconversion de certains médecins généralistes se pose.

Enfin, la loi Santé a été évoquée. Au niveau de l'ANDRH, nous en avons une certaine méconnaissance. Nous estimons pertinent de connecter les questions de la médecine du travail, de la santé publique et de la médecine générale, mais nous nous interrogeons sur la mise en œuvre d'une telle loi. Nous sommes favorables à la prévention et à la lutte contre la désinsertion, mais comment organiser la visite des 45 ans à mi-carrière, alors que les médecins du travail ne sont pas assez nombreux. Les services de prévention et de santé au travail doivent nous proposer différents interlocuteurs. Or, dans les faits, ce principe est difficilement mis en œuvre. Comme vous, nous nous interrogeons souvent sur son coût.

### **Mme Bénédicte Moutin**

Nous avons longtemps considéré que la médecine du travail devait réaliser des visites médicales d'aptitude. Or, la cotisation inclut la prévention et l'accompagnement de l'entreprise.

Des inégalités ont été constatées en fonction des services de santé au travail. L'évolution de l'accompagnement des entreprises représente un enjeu majeur et doit s'appuyer sur les certifications pour encourager la

prévention et garantir un meilleur suivi des salariés au regard des risques encourus dans l'entreprise.

En contrepartie de sa cotisation, l'employeur attend une visite individuelle pour ses salariés. Or ils peuvent solliciter les services de santé au travail pour un éventail de prestations beaucoup plus large. Il a peut-être manqué de pédagogie d'accompagnement des entreprises sur les dernières années.

**Mme Dominique Vérien, Vice-Présidente de la Délégation aux Droits des femmes du Sénat**

Vous avez évoqué les nouveaux modes de travail et le travail indépendant, mais vous n'avez pas évoqué les algorithmes qui entrent dans la gestion des ressources humaines des entreprises. Or les entreprises utilisatrices n'en maîtrisent parfaitement ni le contenu ni les biais. Les biais humains laissent place au diagnostic d'une machine. Dans ce contexte, les femmes sont discriminées négativement, car l'intelligence artificielle ne permet pas de mettre en parallèle des compétences et des durées de connexion.

**M. Matthieu Pavageau**

L'ubérisation et le management algorithmique ont des effets en matière de prescription du travail. La spécificité du travailleur n'est pas prise en compte dans ces modèles qui sont problématiques, car ils ne s'intéressent qu'à la distribution des tâches et à la force de production.

Un accord européen relatif à la transformation numérique a été signé en 2020. Il met en évidence l'urgence de faire monter en compétences tous les acteurs, notamment ceux qui produisent du droit et des accords dans les entreprises, car notre pouvoir de régulation est très faible.

**M. Jean-Emmanuel Ray**

Je fais partie de la commission Frouin sur les plateformes. L'algorithme est le trésor des plateformes de mobilité, car il garantit leur compétitivité. En matière de secret des affaires, sa protection se conçoit aisément.

Par ailleurs, je dois reconnaître que la compréhension des algorithmes demande un effort important aux juristes comme moi.

**M. Didier Dessassis**

Je suis chef d'entreprise et je suis président de l'association de prévention de santé au travail d'Indre-et-Loire. J'estime que les orientations de la nouvelle loi sont pertinentes, mais nous n'avons pas de médecins. Or la réforme ne pourra pas être appliquée sans médecins ni réforme du travail du médecin.

J'estime nécessaire de donner aux SPST les moyens de réaliser leur travail ; de revoir le fonctionnement des centres, car il est difficile de *manager* les médecins ; et d'engager une grande réflexion pour faire avancer le monde du travail par les médecins du travail.

### **Une intervenante**

En tant que chefs d'entreprise, nous devons payer chaque année pour la santé au travail de tous nos salariés alors qu'ils se rendent à une visite tous les cinq ans. Nous devons en outre respecter une sectorisation géographique qui nous interdit de choisir une société de santé au travail en laquelle nous avons confiance.

### **M. Emmanuel Cugny**

Merci pour votre participation, votre pertinence et les nombreuses informations que vous avez échangées.

*La séance est levée à 12 heures 41.*