PREISKEL & CO

COMMENT TRAVAILLER DANS UN MONDE POST-CORONAVIRUS ?

ENABLING BUSINESS IN A POST CORONAVIRUS WORLD

POST COVID-19 : L'AVENEMENT DU DROIT DU TRAVAIL NUMERIQUE

- Avec la crise sanitaire liée à la Covid-19, c'est une nouvelle organisation du travail, l'utilisation de nouveaux outils qui nous ont été imposées : recours massif au télétravail, tenue des assemblées et réunions obligatoires par vidéoconférence, réalisation de signatures électroniques, dématérialisation accélérée des infrastructures…
- A l'heure du déconfinement, les différentes solutions technologiques qui s'offrent aux entreprises pour redresser leur activité économique doivent nécessairement s'accompagner de mesures visant à assurer leur sécurité juridique et technique, afin, notamment, de protéger les systèmes d'information et les données traitées.
- Comment travailler dans un monde post-coronavirus ? Est-il souhaitable de généraliser et de pérenniser certaines des mesures prises pendant le confinement ? Quels sont les risques associés et comment s'en prémunir ? Quelles mesures concrètes ont été prises dans les différents pays dans le monde pour permettre aux entreprises de continuer à travailler ? Plus généralement, quels enseignements tirer de cette période pour construire un avenir durable dans le monde d'après ?

Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde. Les pays suivants ont contribué à ce numéro : Afrique du Sud, Australie, Belgique, France, Grèce, Maroc, Sénégal.

POST COVID-19: LABOUR LAW ENTERS THE DIGITAL AGE

- *With the health crisis linked to the Covid-19 outbreak, we have been forced to adopt a new working organisation and use new tools: working from home, holding mandatory assemblies and meetings by videoconference, implementing electronic signatures, accelerating digital transformation…*
- *As Covid-19-lockdown and stay-at-home orders are ending, the various technological solutions available to businesses to recover their economic activity must necessarily be accompanied by measures to ensure their legal and technical security, and in particular guarantee the security of their information systems and data.*
- *How to enable business in a post coronavirus world? Is it desirable to expand and continue to apply some of the measures taken during the lockdown periods? What are the associated risks and how can they be avoided? What concrete measures have been taken in various countries in the world to enable business? More generally, what lessons can be learned from this period to pave the way for a sustainable future in the world after Covid-19?*

The Lexing® network members provide a snapshot of the current state of play worldwide. The following countries have contributed to this issue: Australia, Belgium, France, Greece, Morocco, Senegal, South Africa.

Lexing®

Lexing® est le premier réseau international d'avocats en droit du numérique et des technologies avancées. Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leurs pays respectifs.

Lexing® is the first international lawyers' network for digital and emerging law. Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

https://lexing.network

EMMANUEL WALLE
Directeur du département droit social numérique du cabinet Lexing Alain Bensoussan-Avocats

Head of Employment Law department of Lexing Alain Bensoussan-Avocats

LEXING ALAIN BENSOUSSAN AVOCATS

▪ La pandémie de Covid-19 a touché de plein fouet l'ensemble des pays dans le monde. Les mesures d'arrêt de l'activité prises pour l'enrayer ont plongé l'économie mondiale dans une récession. Face à la crise, les entreprises ont dû lutter pour assurer tant bien que mal la continuité de leur fonctionnement. De nombreux pays tentent désormais de revenir à une existence normale, après avoir subi le confinement total de leur population. Or, redonner aux citoyens leur liberté tout en contenant le virus est exercice périlleux.

▪ Les conséquences de cette crise vont se faire sentir à long terme et il est donc absolument nécessaire de permettre aux entreprises de se maintenir à flot dans le monde post-coronavirus. A défaut, c'est le virus qui gagne. Alors, comment permettre aux entreprises de survivre ? Est-il souhaitable de généraliser et de pérenniser certaines des mesures prises pendant le confinement ?

▪ En effet, certaines mesures prises au plus fort de la crise afin, par l'auto-isolement et la distanciation physique, de limiter au plus vite la propagation du virus, présentent des avantages à long terme pour les entreprises, tels qu'une productivité accrue, une diminution de la rotation du personnel et une réduction du stress. Quoi qu'il en soit, que ces mesures soient appliquées pour prévenir la transmission de la Covid-19 ou pour d'autres raisons, il est essentiel de ne pas en ignorer les implications juridiques.

▪ Les entreprises se doivent de maîtriser ces différentes mesures afin d'entrer de plain-pied dans le monde d'après.

Utiliser la signature électronique en toute légalité

▪ En Afrique du Sud, la signature électronique est encadrée par la loi ECT (1). Elle est légale pour de nombreux types de transactions. Il est important, pour l'utiliser en toute sécurité, d'en comprendre les concepts clés d'identité, d'intention et de force probante (2).

▪ La signature électronique garantit généralement l'identité du signataire au moyen d'identifiants uniques qui lui sont spécifiquement transmis (URLs spécifiques ou codes PIN uniques envoyés par courrier électronique ou SMS) ou assignés (noms d'utilisateur et mots de passe pour se connecter à un module de signature).

(1) https://www.michalsons.com/blog/guide-to-the-ect-act/81

(2) https://www.michalsons.com/blog/how-to-use-electronic-signatures-securely/43260

▪ Une signature électronique doit être liée aux données destinées à être signées afin de prouver valablement l'accord avec les données d'un fichier électronique ou leur adoption. Elle doit montrer l'intention du signataire d'utiliser sa signature dans ce contexte particulier.

▪ Le niveau de garantie offert par la signature électronique quant à l'identité et l'intention du signataire est renforcé par le recours à des technologies telles que l'authentification multifacteur (pour établir que le signataire est bien celui qu'il prétend être) et le chiffrement (pour prouver, par un artefact de preuve inviolable, que le signataire a bien signé le document électronique). Grâce à ces technologies, il est possible de retracer les étapes qui ont conduit à la signature (la méthode
d'authentification de l'identité des signataires, l'heure exacte de la signature, les modalités choisies pour apposer les signatures).

Travailler à distance en toute sécurité

▪ Avec le télétravail, vos employés travaillent depuis leur domicile ou un autre endroit situé hors des murs de l'entreprise en utilisant internet, le téléphone ou d'autres formes de télécommunication. Comment faire en sorte que votre personnel puisse télétravailler sans compromettre la cybersécurité de votre entreprise ?

▪ La loi sur la cybersécurité de portée générale la plus importante en Afrique du Sud est la loi POPIA (3). Cette loi n'a pas encore été pleinement mise en œuvre (4) mais lorsqu'elle le sera, elle obligera toute personne qui procède au traitement les données à caractère personnel à prendre « des mesures techniques et organisationnelles appropriées et raisonnables » pour les protéger contre tout accès non autorisé.

▪ Dans le domaine du télétravail, les « mesures techniques et organisationnelles appropriées et raisonnables » peuvent se matérialiser par des politiques (5) et des mesures de sécurité complémentaires. Par exemple, une politique de télétravail pourrait définir les exigences relatives à ce type de travail en tenant compte des éléments suivants :

1. les dangers liés à l'utilisation par les employés de leurs propres locaux ;
2. les exigences en matière de sécurité des communications ;
3. les exigences en matière de sécurité numérique ; et
4. les risques liés à l'utilisation par les employés de leur propre matériel.

▪ En ce qui concerne les mesures de sécurité, votre entreprise doit veiller à :

1. fournir à votre personnel l'équipement nécessaire au travail à distance ;
2. définir des règles de travail à domicile ;
3. mettre en place une infrastructure de communication ;
4. assurer la sécurité physique de l'espace et de l'équipement de travail de votre personnel ;
5. établir des règles et des directives pour les familles et les visiteurs de votre personnel concernant l'accès à l'équipement et aux informations de l'entreprise ; et
6. instaurer des procédures pour le changement des contrôles d'accès et la restitution des matériels lorsque votre personnel cesse de travailler à distance.

Dématérialiser vos réunions

▪ Il est possible d'économiser du temps et de l'argent en assurant le fonctionnement et la gouvernance de votre entreprise par voie électronique (6). Vous pouvez ainsi décider de vous réunir en utilisant les communications électroniques et de signer les résolutions prises au cours de ces réunions par voie électronique.

Dématérialiser vos activités et assurer votre présence en ligne

▪ Vous pouvez dématérialiser vos activités et ouvrir un magasin (ou établir une présence) dans le monde virtuel pour compléter votre présence dans le monde réel. Prenez-garde, cependant, à gérer les risques juridiques associés : votre site devra, notamment, intégrer une notice légale (7).

(3) https://www.michalsons.com/ blog/a-practical-approach-to- implementing-popi/9490

(4) Le président d'Afrique du Sud a proclamé l'entrée en vigueur de la POPIA au 1er juillet 2020. Les organismes ont 12 mois à compter de cette date pour se conformer à la POPIA. https://www.michalsons.com/blog/popia-is-here-now-what-the-questions-to-ask/41733

(5) https://www.michalsons.com/l egal-services/legal-documents/policies-and-procedures-getting-them-right

(6) https://www.michalsons.com/ blog/implement-the-companies-act-electronically/2565

(7) https://www.michalsons.com/ focus-areas/internet-law-internet-regulation/legal-notices-for-an-online-store

JOHN GILES
&
DAVID LUYT

south-africa@lexing.network

▪ *The coronavirus and Covid-19 have caused havoc, made countries lockdown, plunged economies into recession and made it very hard for business to continue. Organisations have struggled to continue their operations and do business. Many countries in the world are trying to find their way from a total lockdown back to a normal existence. It's a tight rope walk between giving people back their freedom and containing the virus. Organisations are going to find it hard to operate for some time to come.*

▪ *It is crucial that we find a way to enable business to survive in a post coronavirus world because the effects are going to be with us for some time to come. If we don't, the virus wins. So, how can we enable business? What practices have we developed that might be here for good?*

▪ *These practices are necessities for limiting the spread of the virus in the short-term by enabling self-isolation and social distancing, but they also have many other long-term benefits – such as increased productivity, lower staff turnover and lower levels of stress. But, whether you want to take advantage of having your employees implement these practices to prevent the transmission of Covid-19 or for other reasons – you can't afford to ignore the legal implications.*

▪ *They are a critical part of our commercial lives in a post coronavirus world. They are a vital business and life skill.*

Use electronic signatures lawfully

▪ *Electronic signatures are regulated by the ECT Act (1) in South Africa. They are lawful for many kinds of transactions, but it's important to understand the key concepts of identity, intent and evidential weight to use them securely (2).*

▪ *Electronic signatures typically indicate the identity of the signatory through unique identifiers sent specifically to them (such as specific URLs or one-time-PINs sent to them by email or text message) or unique credentials (such as usernames and passwords to log into a signing dashboard).*

▪ *An electronic signature must be linked to the data intended to be signed to validly evidence agreement with or adoption of data in an electronic record. It should show that signatory intended the signature to be their signature in a particular context.*

▪ *Electronic signatures have greater capacity to positively prove identity and intent by using technologies, such as multi-factor authentication to establish that the signatory is who they claim to be and cryptography to prove that they signed the electronic record by creating a tamper-proof evidentiary artifact. These can confirm the steps that lead up to their signature (such as how the signatories' identity was authenticated and when and how they chose to apply their signature).*

Work remotely but securely

▪ *How do you have personnel work from anywhere (including home) without compromising cybersecurity? This practice is also known as telecommuting, and involves your personnel working from their houses, flats or another location remote*

(1) https://www.michalsons.com/blog/guide-to-the-ect-act/81

(2) https://www.michalsons.com/blog/how-to-use-electronic-signatures-securely/43260

from the office using the Internet, telephone and other forms of telecommunication.

▪ *South Africa's most pervasive cybersecurity law is POPIA (3), but it hasn't commenced fully yet (4). When it does, it will oblige anyone who processes the personal data of data subjects to implement "appropriate and reasonable technical and organisational measures" to protect it from unauthorised access.*

▪ *When it comes to telecommuting, 'appropriate and reasonable technical and organisational measures' would include both policies (5) and supporting security measures. A work from anywhere policy should set out requirements for working from anywhere by considering the:*

1. *dangers associated with personnel using their own premises;*
2. *communications security requirements of how your personnel will be working remotely;*
3. *digital security requirements for your personnel working remotely; and*
4. *risks associated with personnel using their own equipment.*

▪ *When it comes to security measures, your organisation should consider:*

5. *providing workstation equipment to your personnel for working remotely;*
6. *defining working from home rules for your organisation;*
7. *providing communication infrastructure;*
8. *physical security of your personnel's space and equipment;*
9. *family and visitor rules and guidance for access to equipment and information; and*
10. *access control changes and return of equipment when your personnel stop working remotely.*

Administer companies electronically

▪ *We can save time and money, and keep our companies running by administering them electronically (6). We can meet using electronic communications and we can sign resolutions electronically.*

Start an online store

▪ *We need to go online and open an online store (or presence) to supplement our physical presence. But we must manage the legal risks. You need to have the right legal notices (7).*

(3) https://www.michalsons.com/ blog/a-practical-approach-to- implementing-popi/9490

(4) The President of South Africa proclaimed that the Protection of Personal Information Act (POPI Act or POPIA) commenced on 1 July 2020. This means that you have 12 months from that date to comply with POPIA. https://www.michalsons.com/blog/popia-is-here-now-what-the-questions-to-ask/41733

(5) https://www.michalsons.com/l egal-services/legal-documents/policies-and-procedures-getting-them-right

(6) https://www.michalsons.com/ blog/implement-the-companies-act-electronically/2565

(7) https://www.michalsons.com/ focus-areas/internet-law-internet-regulation/legal-notices-for-an-online-store

JOHN GILES
&
DAVID LUYT

south-africa@lexing.network

COVID-19 | Assouplissement temporaire des règles de signature électronique par les entreprises

▪ Afin d'aider les entreprises à poursuivre leurs activités pendant la période de la Covid-19 et à atténuer l'impact économique de cette la pandémie, le ministre de l'économie et des finances a assoupli les dispositions de l'article 127 de la loi sur les sociétés de 2001 fixant les conditions de validité de la signature de documents par une société, de telle manière à ce que cette signature puisse se faire par voie électronique et sur des documents distincts en cas de pluralité de signataires.

▪ Cet assouplissement temporaire est valable six mois à compter du 6 mai 2020. Il s'inscrit dans le cadre de la Décision (n°1) 2020 sur la réponse économique au Coronavirus (1), prise par la ministre en vertu des pouvoirs qui lui ont été conférés par la nouvelle section 1362A de la loi sur les sociétés de 2001, récemment insérée en vue de faire face à la situation créée par la Covid-19. La Décision (n°1) 2020 modifie par ailleurs également d'autres dispositions de la loi sur les sociétés de 2001, ainsi que le règlement sur les sociétés de 2001, les règles relatives aux pratiques en matière d'insolvabilité et les règles relatives aux passeports financiers.

(1) Corporations (Coronavirus Economic Response) Determination (No. 1) 2020

Signature de documents

▪ La section 127 de la loi sur les sociétés de 2001 conditionne la validité de la signature d'un document, dans le cas où l'entreprise n'utilise pas de cachet, à la signature manuscrite de deux administrateurs, ou d'un administrateur et d'un secrétaire général, ou de l'administrateur unique en cas de sociétés constituées d'un seul administrateur. La Décision (n°1) 2020 modifie temporairement cette section 127 en reconnaissant que :

- la signature peut également être électronique, et
- en cas de pluralité de signataires (par exemple deux administrateurs), leurs signatures ne doivent pas nécessairement être apposées sur le même document, chacun pouvant appliquer sa signature sur une copie ou une exemplaire original,

à condition que la copie, l'exemplaire original ou la communication électronique inclut l'intégralité du contenu du document. Lorsque les documents se présentent sous forme de communication électronique, la Décision (n°1) 2020 reprend expressément certaines exigences figurant dans la loi sur les transactions électroniques de 1999 (2). Ces exigences sont satisfaites :

- si une méthode est utilisée pour identifier la partie et pour indiquer la volonté de cette partie concernant l'information contenue dans la communication électronique ; et

(2) Electronic Transactions Act 1999

- si la méthode utilisée est :
  - soit une méthode dont la fiabilité est suffisante au regard de l'objet pour lequel la communication électronique est signée, compte tenu de toutes les circonstances, y compris toute convention en la matière ;

- soit une méthode dont il est démontré dans les faits qu'elle a, par elle-même ou avec d'autres preuves, rempli les fonctions visées à l'alinéa ci-dessus.

▪ Alors que l'on vient de fêter le 20e anniversaire de l'entrée en vigueur de la loi sur les transactions électroniques, d'aucuns diront que son actualisation se fait attendre. Cette loi, qui a pour but de garantir la validité des documents établis et signés électroniquement, avait été qualifiée de progressiste à l'époque, mais la loi sur les sociétés avait été spécifiquement exclue de son champ d'application.

▪ La Décision (n°1) 2020 représente donc une évolution majeure. Si les sociétés peuvent signer des contrats par d'autres moyens (sous réserve des dispositions de leurs statuts), y compris par voie électronique, la signature spécifiquement visée à la section 127 de la loi sur les sociétés de 2001 est particulièrement importante car elle permet généralement à la partie contractante de bénéficier d'une présomption légale de validité de la signature, en vertu des sections 128 et 129 de cette même loi.

▪ En conséquence, il est recommandé aux entreprises de prendre les mesures immédiates suivantes :

- Passer en revue les protocoles de signature applicables au sein du conseil d'administration ainsi que les conditions à respecter par les administrateurs et les secrétaires généraux afin d'être autorisés à signer des documents. Étant donné qu'une partie contractante est en droit de se prévaloir de la présomption de validité des signatures apposées sur un document, le conseil d'administration devrait s'assurer de disposer de contrôles internes adéquats à cet égard.
- Être conscient du fait qu'il sera potentiellement plus facile pour un tiers, que ce soit par malveillance ou en toute bonne foi, de signer un document au nom d'un dirigeant de la société, et pour la signature ainsi apposée sur ce document de bénéficier de la présomption légale de validité. Même si cette question n'est pas inconnue des tribunaux, cette présomption légale risque de constituer un terreau fertile au développement de litiges.
- Veiller à ce que les noms et coordonnées de ses dirigeants enregistrés auprès de l'ASIC, l'autorité australienne des marchés financiers, et publiquement disponibles, soient bien à jour. En effet, la section 129 de la loi sur les sociétés dispose que toute personne peut supposer que les personnes ainsi indiquées ont été valablement nommées et détiennent les pouvoirs nécessaires. Il existe donc un risque, rendu encore plus accu par la Décision (n°1) 2020, que l'indication de mauvaises personnes auprès de l'ASIC puisse exposer la société à se voir liée par des contrats non désirés.

Pistes de réflexions

▪ Les changements mis en œuvre pour faciliter les signatures électroniques offrent une plus grande flexibilité aux entreprises touchées par la Covid-19.

▪ Bien que la Décision (n°1) 2020, prise pour répondre aux besoins crées par la Covid-19, n'ait d'effet que pendant six mois, nombreux sont ceux qui espèrent que ses dispositions deviendront, d'une manière ou d'une autre, permanentes et aboutissent à une modification de la loi sur les sociétés de 2001.

DUDLEY KNELLER

australia@lexing.network

COVID-19 | Electronic signing: New temporary relief for companies a significant step on a longer journey

▪ *In a significant development for companies, the Treasurer has utilised his new power to modify the Corporations Act 2001, the Corporations Regulations 2001, the Insolvency Practice rules, and the Passport Rules so that, for a period of six months effective from 6 May 2020 execution of documents by a company for the purpose of section 127 of the Act may be done so electronically and, where there are two signatories, on separate documents.*

▪ *The Treasurer has exercised these powers through the issuing of Corporations (Coronavirus Economic Response) Determination (No. 1) 2020, pursuant to his new powers afforded under the recently installed section 1362A of the Act to respond to the Covid-19 situation.*

Execution of documents

▪ *The Determination amends the Corporations Act to confirm that valid execution of a document, without a common seal, for the purpose of section 127 of the Act, whether by two directors, a director and company secretary or, in the case of sole director/secretary companies, that person:*

- *can be done so electronically, rather than with "wet ink";and*
- *where there are two signatories (e.g. two directors), their signatures do not need to be applied to the same document but can do so by each applying their respective signatures to a copy orcounterpart,*

provided that the copy, counterpart or electronic communication includes the entire contents of the document. In the context of documents that are electronic communications, certain principles found in the Electronic Transactions Act 1999 have been expressly included in the Determination, namely that, in respect of an electronic communication:

- *it uses a method to identify the person and to indicate the person's intention in respect of the contents of the document; and*
- *the method:*
  - *is as reliable as appropriate for the purpose, in light of all the circumstances, including any relevant agreement; or*
  - *is proven in fact to have fulfilled the functions described above, by itself or together with further evidence.*

▪ *With the 20th anniversary of the commencement of the Electronic Transactions Act having recently passed, many will say that these changes are a long time coming. While the Electronic Transactions Act was progressive at the time in seeking to provide assurance of the validity of documents made and signed electronically, the Corporations Act has specifically been excluded from the effect of that legislation.*

▪ *This Determination is therefore a significant development. While companies have been able to sign contracts in other ways (subject to their governing*

document) including electronically, execution under section 127 is particularly important because it usually will afford the counterparty the benefit of a statutory assumption, by virtue of sections 128 and 129, that the document has been validly executed.

▪ *Arising from this, the immediate action items for companies are likely to include the following:*

- *Reviewing board execution protocols and the manner by which directors and company secretaries are authorised to execute documents. Given that a counterparty is entitled to assume a document bearing relevant signatures has been validly executed, the board should consider whether it has adequate internal controls in this regard.*
- *In particular, it will potentially be easier for a third party, whether maliciously or in good faith, to execute a document in the name of a company officer and for that document to carry the burden of the statutory assumption of valid execution. While the courts have explored this issue somewhat, the impact of the statutory assumption will create fertile ground for litigation.*
- *Ensuring details of its officers recorded with ASIC remain current. Section 129 of the Corporations Act states that where there is information publicly available from ASIC as to directors and secretaries of a company, derived from information provided by the company, a person may assume that such people have been validly appointed and hold due authority. As has always been the case, and now heightened by the potential outcomes from this Determination, having the wrong people recorded with ASIC could lead to undesirable outcomes for a company burdened with an unwanted contract.*

Final thoughts

▪ *The changes implemented to permit electronic signatures provide greater flexibility to the impacted Covid-19 business community.*

▪ *Though the Determination only has effect for six months, and can only be made where the Treasurer is satisfied that it is necessary to respond to the impact of Covid-19, many will be hoping this paves the way for amendments to the Corporations Act itself in due course and for these arrangements to become permanent in some fashion.*

DUDLEY KNELLER

australia@lexing.network

▪ La pandémie de la Covid-19 et les mesures de confinement décidées en Belgique ont rendu obligatoire le recours au télétravail pendant plusieurs semaines. Le télétravail, essayer, c'est l'adopter ? La réponse est incontestablement positive. Toutefois, l'intégration du télétravail comme mode d'organisation du travail au sein d'une entreprise doit être réfléchie et réglementée.

▪ La réflexion doit débuter autour de la notion même de télétravail. En effet, cette notion, dans sa définition commune, vise les prestations effectuées au départ d'un lieu autre que les bureaux de l'entreprise, à savoir le lieu de résidence du travailleur. Légalement, cette notion doit être nuancée et trois concepts doivent être distingués :

- le télétravail structurel,
- le télétravail occasionnel,
- le « homeworking ».

▪ En pratique, le télétravail organisé à concurrence, par exemple, de deux jours par semaine est du télétravail structurel. Le télétravail autorisé lorsqu'un travailleur doit se rendre, par exemple, à un rendez-vous médical ou lors d'une grève des transports est du télétravail occasionnel. Enfin, la possibilité donnée à un travailleur de rester chez lui, par exemple, pour travailler un projet nécessitant une concentration particulière ne correspond à aucune des deux catégories précédentes. Nous décidons de l'appeler « homeworking ».

▪ Selon la catégorie - légale - de télétravail, les droits et obligations des employeurs et des travailleurs diffèrent. Un principe général se dégage toutefois : la mise en place du télétravail au sein d'une entreprise - quelle que soit sa qualification - doit résulter d'un accord entre employeur et travailleur. En d'autres termes, l'employeur ne peut l'imposer, le travailleur ne peut l'exiger.

Le télétravail structurel

▪ Le télétravail structurel est régi par la CCT n° 85 du 9 novembre 2005 concernant le télétravail. Cette convention collective oblige l'établissement d'une convention écrite individuelle dans laquelle sept mentions obligatoires doivent apparaître :

1. la fréquence du télétravail – éventuellement les jours télétravail/présentiel
2. les conditions de travail
3. les moments ou périodes durant lesquels le télétravailleur doit être joignable et suivants quels moyens
4. les moments où le télétravailleur peut faire appel à un support technique
5. les modalités de prise en charge des frais et des coûts. La prise en charge des coûts liés au télétravail structurel par l'employeur est obligatoire. Le texte légal ne définit toutefois pas les coûts qui doivent être assumés par l'employeur. Nous vous conseillons donc de déterminer précisément les frais pris en charge, ce qui exclura toute revendication ultérieure.
6. les conditions et modalité d'un retour au travail
7. le(s) lieu(x) où le télétravail est exécuté

▪ Toute autre mention est facultative. Il est conseillé de modaliser par écrit d'autres éléments et notamment les méthodes d'évaluation des prestations par la fixation d'objectifs par exemple, les mesures applicables en cas de force majeure (exemple : coupure internet) puisque le paiement de la rémunération, même en

cas de force majeure, est obligatoire. Outre l'établissement d'une convention écrite, différentes obligations sont à charge de l'employeur concernant le bien-être au travail, la fourniture du matériel, d'un service technique et la mise en place d'un système de protection des données.

▪ Le travailleur a, quant à lui, l'obligation de prendre soin des équipements lui confiés et d'informer l'employeur en cas d'impossibilité de prester.

Le télétravail occasionnel

▪ Le télétravail occasionnel est régi par les articles 22 et s. de la loi du 5 mars 2017 concernant le travail faisable et maniable. Le télétravail occasionnel se justifie lorsque que le travailleur est empêché d'effectuer ses prestations dans les locaux de l'entreprise, soit dans deux hypothèses :

- en cas de force majeure,
- pour raisons personnelles.

▪ Le télétravail occasionnel n'est autorisé que pour les fonctions dont la nature est conciliable avec le télétravail. Le travailleur doit introduire une demande préalable dans un délai raisonnable en indiquant le motif. L'employeur peut refuser la demande. Le refus doit être notifié par écrit.

▪ Les parties doivent s'entendre sur trois points :

- la mise à disposition éventuelle par l'employeur de l'équipement nécessaire et le support technique,
- l'éventuelle accessibilité du travailleur pendant le télétravail,
- la prise en charge éventuelle des frais.

▪ Il n'est pas obligatoire de fixer les modalités du télétravail occasionnel dans une convention écrite. Nous vous conseillons toutefois de fixer un cadre déterminant les fonctions/activités compatibles, la procédure de demande d'autorisation, la mise à disposition des équipements, l'accessibilité du travailleur et la prise – ou non prise - en charge des frais.

Le homeworking

▪ Dans certaines circonstances, l'autorisation de télétravailler peut s'avérer utile à l'entreprise, sans que les prestations effectuées ne correspondent aux définitions légales de télétravail structurel ou occasionnel. Nous pensons notamment à la nécessité de permettre à un travailleur de pouvoir se concentrer sur un travail défini sans être distrait par la vie de l'entreprise (réunions, appels téléphoniques, interpellations de collègues…).

▪ Dans cette hypothèse et puisqu'il ne s'agit ni d'un cas où le travailleur est empêché de prester au départ de l'entreprise en raison d'un cas de force majeure ou pour raisons personnelles, ni d'une forme d'organisation du travail planifiée de manière régulière dans le temps, aucune réglementation ne trouve à s'appliquer. Une nouvelles fois, nous vous conseillons de modaliser le recours à cette forme d'organisation du travail par écrit et ce, pour éviter toute difficulté dans sa mise en œuvre.

En conclusion

▪ Le télétravail est un concept à géométrie variable qui peut s'adapter aux besoins de l'entreprise. Dès lors que le télétravail ne peut être imposé ni par l'employeur, ni par le travailleur, que selon les conséquences varient selon la formule choisie, sa mise en œuvre doit faire l'objet d'une réflexion et d'une réglementation interne à l'entreprise.

WIVINE SAINT-REMY

belgium@lexing.network

▪ *The Covid-19 pandemic and the lockdown measures decided in Belgium have made teleworking compulsory for several weeks. Were employees happy with such teleworking experience? The answer is unquestionably yes. If your company is now considering definitely integrating telework into your working organisation, you need to adopt a strategy and establish appropriate policies.*

▪ *First, you need to carefully consider the very concept of 'telework'. In its ordinary meaning, it refers to services provided from a place other than the company's offices, i.e. from the employee's place of residence. In its legal meaning, it can be divided into three categories:*

- *structural telework,*
- *occasional telework,*
- *homeworking.*

▪ *In practice, organized telework up to, for example, two days a week is structural telework. Telework that is authorized when an employee has to go to a medical appointment or during a transport strike, for example, is occasional telework. The possibility given to an employee to stay at home, for example, to work on a project requiring a particular focus does not fit into either of the previous two categories; we will call it "homeworking".*

▪ *Depending on the (legal) category of telework, the rights and obligations of employers and employees are not the same. A general principle stands out, tough: the introduction of telework within a company— whatever its category — must be the result of an agreement between the employer and the employee. In other words, the employer cannot impose it and the employee cannot demand it.*

Structural telework

▪ *In Belgium, structural telework is governed by the collective labour agreement (CCT) No. 85 of 9 November 2005 on telework. This collective agreement requires an individual written agreement which must contain the following seven mandatory items:*

1. *The frequency of telework (telework days/presence days)*
2. *The working conditions*
3. *The times or periods during which the remote worker must be reachable and by what means*
4. *The times when the remote worker can call for technical support*
5. *The arrangements about fees and costs. The employer must bear the costs of structural telework. The CCT does not detail the costs to be borne by the employer. To avoid any conflict, it is advisable to clearly state the exact costs that will be covered*
6. *The terms and conditions of a return to work*
7. *The location(s) where telework is performed*

▪ *Any other information is optional. It is, however, recommended to establish in writing other items, such as the methods for evaluating the services performed (e.g. in relation to objectives set), the measures applicable in case of force majeure (e.g. internet outage) since the payment of the remote worker's remuneration is mandatory, even in case of force majeure. In addition to the establishment of a*

written agreement, various other obligations are imposed on the employer such as ensuring well-being at work, providing equipment, providing technical support service and setting up a data protection system.

▪ *Employees are required to take care of the equipment entrusted to them and to inform their employer if they are unable to work.*

Occasional telework

▪ *Occasional telework is governed by articles 22 et seq. of the Law of 5 March 2017 concerning feasible and manageable work. Occasional telework is justified when the worker is prevented from working on the company's premises, in two cases:*

- *in the event of force majeure,*
- *for personal reasons.*

▪ *Occasional telework is only allowed for tasks that are compatible with telework. The employee must submit a prior request within a reasonable period of time stating the reason for telework. The employer may refuse the request. Refusal must be notified in writing.*

▪ *The parties must agree on three points:*

- *whether the employer provides the necessary equipment and technical support,*
- *whether and how the employee may be reached during telework,*
- *who will pay the costs.*

▪ *It is not mandatory to set out the terms and conditions of occasional telework in a written agreement. However, we advise you to establish a framework determining the list of compatible jobs/activities, the procedure for filing a telework authorisation form, the procedure for providing/returning equipment, the employee's availability hours, and the payment (or non-payment) of costs.*

Homeworking

▪ *In certain circumstances, telework may be useful for the company, even if the services performed do not meet the legal definitions of structural or occasional telework. This includes situations where an employee needs to concentrate on a specific job without being distracted by the company's routine activities (such as meetings, telephone calls, questions from colleagues).*

▪ *In this case, and since it is neither a case where the worker is prevented from working in the company premises because of force majeure or personal reasons, nor a form of work organisation planned on a regular basis over time, no specific regulation is applicable. Once again, to avoid any difficulties, we advise you to set out the details of such work organisation in writing.*

Conclusion

▪ *Telework is a living concept that can be adapted to the needs of the company. As telework cannot be imposed either by the employer or by the employee, and since the consequences vary according to the type of telework chosen, its implementation must be thoroughly thought through and give rise to company policies.*

WIVINE SAINT-REMY

belgium@lexing.network

Post Covid-19 : l'avènement du droit du travail numérique

▪ La crise sanitaire a poussé plusieurs millions de Français vers le travail à distance. La perspective d'une deuxième vague associée au ralentissement presque programmé de l'activité économique mondiale, obligent les acteurs que nous sommes à accélérer le traitement juridique des mutations des formes d'emploi et de travail.

▪ Que pouvons-nous constater ? En France, le dogme du salariat n'apparait plus comme une solution mais comme devant se combiner avec d'autres modes d'organisation du travail, facilité notamment par le succès des plateformes numériques que le vocable « d'ubérisation » a popularisé.

▪ Les craintes de la destruction du travail par le développement des technologies et la numérisation s'éloignent au contact du principe de réalité qu'a déclenché le séisme de la Covid-19.

▪ Il importe avant tout, non seulement de s'ouvrir le champ des nouveaux emplois induit par les technologies avancées, mais aussi de promouvoir une sécurité juridique multiplicatrice de confiance.

▪ En quelque sorte, la dimension post Covid-19 implique de valoriser les travailleurs numériques, ceux-là même expulsés du système d'avant qui décident de devenir freelance ou autoentrepreneur, en se loguant sur des plateformes d'intermédiation pour louer leurs services et ainsi tenter d'échapper au marécage économique programmé.

▪ L'interrogation est centrale en France, tant les dispositions du code du travail et son exposition prétorienne, demeurent ignorants du reste du monde, des nouvelles formes d'emploi où les moins de 20 ans postent leurs CV sur des plateformes de grandes écoles déterritorialisées. Et pendant ce temps-là, les contentieux nationaux impliquant les services d'Uber ou d'Airbnb se multiplient.

▪ Ce type de contentieux aujourd'hui hissé au niveau communautaire ne doit-il pas voir le monde d'après ?

▪ A l'heure des premiers plans sociaux, il est facile d'observer une tendance déjà amorcée avant la Covid-19, une forte augmentation des freelances et autoentrepreneurs que des plateformes numériques collaboratives accueillent pour les faire matcher avec des pourvoyeurs d'emplois.

▪ Une pluralité de plateformes numériques voit donc le jour pour répondre aux spécificités des statuts et des activités des collaborateurs concernés, non plus pour contourner une situation légale existante contraignante, mais répondre à des exigences nouvelles que sont des modalités de travail différentes.

▪ Après le confinement, les plateformes collaboratives pour ne parler que de ce phénomène, deviennent des outils qui rendent la comparaison des organismes classiques existants, obsolètes, compte tenu des enjeux en cours. Que vaut la présomption de salariat ou les clivages travailleur indépendant/travailleur salarié ?

▪ Il ne convient pas de tout sacrifier sur l'autel du monde d'après. Il appartiendra toujours au juge d'interpréter les conventions litigieuses et de sonder l'intention des acteurs, de dénoncer les employeurs peu scrupuleux qui viendront contourner le droit protecteur des travailleurs.

▪ Pour autant doit-on considérer suspects par nature les entremetteurs 2.0 et les freelances qui se rencontrent dans un espace virtuel ?

▪ Les entreprises qui souhaitent externaliser des pans entiers d'activités en faisant appel à des plateformes d'intermédiation devront-elles alors se tourner vers des Etats plus compréhensifs ?

▪ En ce sens, la décision récente concernant la société Deliveroo vient matérialiser un risque bien français de requalification de l'auto-entreprenariat en salariat. Les conséquences de la Covid-19 devront rebattre certaines cartes et imposer aux acteurs concernés de trouver un nouvel équilibre sous peine de faire supporter à la société encore active des charges bien lourdes.

▪ Il appartient aussi aux avocats que nous sommes de trouver un antidote à des décisions bien pensées dans un univers à l'époque encore sans masque.

▪ Les syndicats, l'inspection du travail, l'Urssaf, les services fiscaux restent campés sur des critères encore flous comme le travail dissimulé ou le prêt de main d'œuvre illicite. Il leur appartiendra aussi d'adapter leur pratique plus que leur réglementation qui, on le sait, dispose d'une plus grande flexibilité.

▪ Le monde du travail va devoir ainsi se montrer à la hauteur des défis qu'engendre un ralentissement mondial de l'économie, trouver des débouchés pour les travailleurs 2.0. La question du statut social du travailleur numérique reste centrale en Europe et le droit « dur » ne devra plus freiner les développements de ces plateformes pour protéger un modèle économique existant : le droit du travail est aussi un droit du travail numérique.

EMMANUEL WALLE

france@lexing.network

Post Covid-19: labour law enters the digital age

▪ *The health crisis has pushed several million French people towards teleworking. The prospect of a second wave associated with the almost programmed slowdown in global economic activity forces us to accelerate the legal treatment of the new forms of employment and work brought about by Covid-19.*

▪ *Where are we now? In France, the dogma of salaried employment no longer appears to be* the *solution but* a *solution to be combined with other modes of working organisation, facilitated in particular by the success of 'uberized' digital platforms.*

▪ *Faced with the principle of reality triggered by the Covid-19 earthquake, fears that technology and digital transformation would destroy jobs have subsided.*

▪ *The priority now is not only to open up the field of new jobs created by advanced technologies, but also to promote the legal security required to increase confidence.*

▪ *In a way, the world after Covid-19 implies valuing digital workers — i.e. the very people who, expelled from the world before Covid-19, decided to become freelancers or self-employed by logging in to intermediation platforms to rent their services and try to escape the programmed economic quagmire.*

▪ *This is a key question in France, as the provisions of the Labour Code and its application by case law still remain ignorant of the rest of the world, of the new forms of employment where the under 20-year-olds upload their resumes on the non-territorial-based platforms of grandes écoles. And meanwhile, national disputes involving the services of Uber or Airbnb are multiplying.*

▪ *Will these types of litigation, now handled at the Community level, survive the world after Covid-19?*

▪ *Amid the job cuts caused by the coronavirus outbreak, a trend that started before Covid-19 is becoming all too clear: a strong increase in freelancers and self-employed people who use collaborative digital platforms to meet with job providers.*

▪ *A variety of digital platforms have emerged to meet the various statuses and activities of their users, who are no longer using such platforms to circumvent an existing restrictive legal situation, but to adapt to new working methods.*

▪ *After the lockdown, collaborative platforms – to speak only of this phenomenon – have become tools that, given the current stakes, make the existing, classical organisations obsolete. What is now the value of the presumption of salaried employment or the self-employed versus salaried worker divide?*

▪ *We should not sacrifice everything on the altar of the world after Covid-19, tough. It will always be up to the judge to interpret litigious agreements and to sound out*

the intention of the parties, and to denounce unscrupulous employers who will try to skirt the laws protecting workers.

▪ *However, should we still continue to regard as suspicious by nature the 2.0 intermediaries and freelancers who meet in a virtual space?*

▪ *Will companies that wish to outsource entire areas of activity using intermediation platforms have to turn to more understanding countries?*

▪ *In this sense, the recent* Deliveroo *ruling exemplifies a very French risk of seeing self-entrepreneurship considered by judges as salaried employment. The consequences of Covid-19 will require to reshuffle certain cards and force all stakeholders to find a new balance; otherwise, those who are still active will have to bear the brunt of the crisis.*

▪ *It is also up to us, lawyers, to find an antidote to decisions that were well-thought-out in a universe that was still unmasked.*

▪ *Trade unions, the labour inspectorate, the Urssaf and tax authorities cling to criteria that are still unclear, such as concealed employment or unlawful loan of labour. It will also be up to them to adapt their practices rather than their regulations, which, as we know, are more flexible.*

▪ *The world of work will thus have to rise to the challenges posed by a global economic slowdown and find opportunities for workers 2.0. The question of the social status of digital workers remains crucial in Europe and hard law should no longer hinder the development of these platforms just to protect an existing business model: labour law must also include digital labour.*

EMMANUEL WALLE

france@lexing.network

▪ Nouvelle réglementation. La Covid-19 a bouleversé le fonctionnement des entreprises dans le monde entier, y compris en Grèce, et modifié la manière dont les organisations appréhendent et mettent en œuvre les technologies de travail à distance. Pour faire face à cette situation, l'État grec a introduit un certain nombre de règlements, notamment dans le domaine des prestations de services et des relations de travail.

▪ Le ministère du travail a ainsi publié une circulaire fixant quatre (4) catégories de mesures de sécurité spéciales à prendre sur le lieu de travail, en vue de protéger l'ensemble des travailleurs, quel que soit leur statut professionnel. Cette circulaire concerne tous les lieux de travail, privés et publics, que leur activité soit actuellement suspendue ou non, et apporte des précisions pour lutter contre la propagation de la Covid-19 en tant que risque professionnel pour les travailleurs en Grèce. Elle s'inscrit dans le prolongement de la législation existante en matière de santé au travail aux termes de laquelle l'employeur, en coordination avec le technicien de sécurité et le médecin du travail (lorsque ce dernier est requis conformément à la loi), est tenu de détecter et d'évaluer les risques professionnels sur le lieu de travail et de prendre les mesures appropriées afin de garantir la sécurité et de protéger la santé des travailleurs.

▪ Parmi les autres mesures de soutien aux entreprises adoptées en Grèce pour faire face à l'épidémie de Covid-19 figure également « Syn-ergasia », un dispositif de chômage partiel financé à hauteur de 1,4 milliard d'euros, qui s'applique au cours de la période allant du 01.06.2020 au 30.09.2020. Toutes les entreprises peuvent bénéficier de ce dispositif à condition de démonter avoir subi une perte de chiffre d'affaires d'un pourcentage fixé par ledit dispositif. Les entreprises bénéficiaires ont le droit de réduire, jusqu'à 50 %, le temps de travail de leurs employés à temps plein, qu'ils soient saisonniers ou non. Les employeurs qui recourent à ce mécanisme continuent toutefois de supporter toutes les cotisations sociales de l'employé dont l'activité est ainsi réduite, calculées sur la base de l'intégralité de son salaire nominal. Dans le même temps, l'État grec prend à sa charge 60 % du montant du salaire correspondant à l'activité réduite, étant précisé que le montant du salaire net du salarié ne peut être inférieur au salaire minimum, tel qu'il est actuellement fixé par la législation grecque. Les employeurs ne peuvent licencier les employés bénéficiant de ce mécanisme ou modifier les conditions de leur contrat.

▪ Réglementation existante. Compte tenu des règles de distanciation physique imposées en raison de la Covid-19, les organisations privées et publiques ont, notamment, eu davantage recours à des solutions de signature numérique pour conclure des contrats et, plus généralement, communiquer à distance (c'est-à-dire, en ligne). A cet égard, il convient de noter que la réglementation pertinente, et notamment le règlement (UE) n°910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement eIDAS) et les infrastructures correspondantes, étaient déjà en place en Grèce.

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

greece@lexing.network

▪ *New regulation. Covid-19 has disturbed operation of businesses globally, also in Greece and has affected the way organisations approach and implement distance working technologies. The Greek State, acting in response to Covid-19, has introduced a number of regulations, covering, inter alia, offering of services and employment relationships.*

▪ *The Ministry of Labor issued a Circular providing four (4) categories of special safety measures to be taken in the workplace, with the aim to protect all workers, regardless their working status. The Circular addresses all workplaces, private and public, suspended and currently operating, and it provides specifications for tackling the spread of Covid-19 as an occupational hazard, on the basis of the existing legislation for occupational health for workers in Greece. According to said legislation, the employer, in coordination with the Safety Technician and the Occupational Doctor (where the latter is needed according to the law), shall detect and evaluate the occupational hazards in the workplace and take the appropriate measures in order to secure safety and protect workers' health.*

▪ *Other measures to support businesses in Greece include "Syn-ergasia", an initiative funded by a program up to €1,4 billion, which shall apply in the period from 01.06.2020 until 30.09.2020. This mechanism is addressed and available to all businesses, which can prove that they have suffered certain turnover loss. Said businesses will have the right to reduce up to 50% the working time of their whole-time employees, either seasonal or not. Employers participating in this mechanism shall cover all insurance contributions of the reduced employee, calculated on the basis of their whole nominal salary. At the same time, the Greek State will cover 60% of the amount of the employee's salary that corresponds to the working time reduction, while the employee's amount of net earnings shall not fall under the minimum wage limit, as currently set by Greek legislation. As far as employees submitted under this mechanism are concerned, employers are restricted from terminate them or amend their contract's terms and conditions.*

▪ *Existing regulation. Social distancing rules imposed due to Covid-19 and the need to conclude agreements and generally formally communicate from distance (online) has notably increased the adoption of digital signature solutions by private and public organisation in support of their day-to-day operations. Relevant regulation, most importantly Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) and relevant infrastructure had already been in place in Greece.*

GEORGE A. BALLAS
&
THEODORE
KONSTANTAKOPOULOS

greece@lexing.network

La signature électronique en droit marocain

▪ Les mesures de distanciation sociale et les restrictions à la libre mobilité des personnes, suite à la propagation de la pandémie de la Covid-19, ont induit un recours accru aux nouvelles technologies de communication, et accéléré le processus de digitalisation de l'administration marocaine ainsi que le recours des opérateurs économiques aux nouvelles technologies de l'information pour assurer la continuité de leurs activités à distance.

▪ Cependant, cette évolution ne peut acquérir un caractère définitif que dans la mesure où le cadre juridique régissant la conclusion des contrats par voie électronique et la signature électronique, le permette et que les modalités de mise en place des procédures nécessaires à cet effet, soient efficientes.

Le cadre juridique de la signature électronique au Maroc

▪ Le processus de dématérialisation des données entamé depuis plusieurs années, dans le sillage de l'essor des nouvelles technologies de communication par voie électronique, demeurait handicapé par l'absence d'un cadre juridique garantissant la validité des contrats établis par voie électronique et la force probante de la signature électronique.

▪ Nonobstant le recours accru à l'échange et au stockage des données par voie électronique, dès que la relation entre les parties devait se traduire par la formalisation d'engagements contractuels, le recours à l'écrit demeurait inévitable.

▪ Aussi, la volonté d'accélérer le développement de ces nouveaux modes de transaction a été rapidement confrontée aux limites du droit civil marocain, fondé sur le principe de la preuve écrite, établi par le DOC (1) et qui ne permettait pas à la signature électronique de produire les effets juridiques équivalents à ceux d'une signature établie sur un support papier.

▪ En l'absence d'une référence légale explicite à la valeur juridique de la signature électronique, en tant qu'outil de vérification de l'identité des parties signataires, ainsi que de l'authenticité du contenu de l'acte contractuel et son rattachement aux parties, son utilisation en tant que preuve de l'existence d'obligations contractuelles n'était pas envisageable (2).

▪ Dans ce contexte, le législateur marocain a adopté le 30/11/2007, la loi n°53-05 concernant l'échange électronique de données juridiques (3), et ayant pour objectif de :

- Fixer le cadre juridique applicable aux données échangées par voie électronique ;
- Consacrer l'équivalence des documents échangés par voie électronique et comportant une signature électronique aux documents établis sur un support papier ;
- Fixer le cadre juridique applicable aux opérations effectuées par les prestataires de certification électronique ;

(1) Dahir des Obligations et des contrats

(2) En effet, conformément aux termes de l'article 417 et 443 du DOC La preuve littérale résulte d'un acte authentique ou d'une écriture sous seing prix et les conventions ayant pour objet la création, le transfert, la modification ou l'extinction d'obligations et de droits dont la valeur excède la somme de dix mille (10.000) dirhams doivent être passées acte authentique ou sous seing privé

(3) S'inspirant des principes généraux de la CNUDCI sur les signatures électroniques de 2001 et de la Directive n°1999/93/CE portant cadre communautaire pour les signatures électronique

- Mettre en place d'une autorité nationale d'agrément et de surveillance.

▪ La promulgation de la loi n°53-05 s'est traduite par la reconnaissance de la valeur juridique de la signature électronique et de sa force probante à travers les articles 417-1 (4) et 417-2 (5) du DOC, lesquels ont confirmé l'équivalence de la preuve établie sur un support électronique à celle établie sur un support écrit et sa force probante.

▪ L'admission de la signature électronique comme preuve de l'établissement d'un acte contractuel est cependant exclue pour tout acte relatif à l'application du code de la famille ou des sûretés personnelles ou réelles de nature civile ou commerciale

▪ La fiabilité de la signature électronique est présumée lorsqu'elle a été établie de manière sécurisée (6).

▪ L'admission de la signature électronique et la consécration de la force probante de l'écrit électronique sont cependant assujettis à certaines conditions posées par le législateur et ayant pour objectif que l'acte concerné soit établi et conservé dans des conditions de nature à garantir l'identité de la personne dont a émané la signature ou le document électronique ainsi que l'intégrité de l'acte juridique concerné.

▪ Ainsi, la reconnaissance de la signature électronique en tant que moyen de preuve est tributaire de l'utilisation d'un procédé fiable d'identification, à savoir, le certificat électronique, garantissant son lien avec l'acte auquel elle s'attache et permettant de :

- vérifier l'identité de l'émetteur ;
- contrôler l'intégrité du contenu ;
- rendre non réfutable un échange ou la signature d'un document ;
- effectuer des échanges confidentiels.

▪ En effet, le législateur a mis en place un dispositif de sécurisation du procédé de création de la signature électronique permettant, à travers un matériel et/ou logiciel destiné à cet effet, d'identifier les éléments distinctifs caractérisant le signataire et nécessaire pour la confirmation du rattachement de la signature électronique à son titulaire

▪ La signature électronique doit être attestée par un certificat de conformité simple ou sécurisé (7).

▪ Afin de doter le système mis en place de la sécurité juridique nécessaire, le législateur a subordonné le droit d'émettre des certificats de signature électronique à l'obtention d'un agrément émis par l'autorité nationale d'agrément et de surveillance de la certification électronique. À ce jour, seul Barid ALMAGHRIB (Poste du Maroc) (8) a été agrée en tant qu'autorité habilitée à émettre un certificat électronique.

Conditions de sécurisation de la signature électronique

▪ La mise en place des règles juridiques permettant de doter la signature électronique de la force probante nécessaire pour qu'elle puisse être utilisée de manière récurrente tant par des administrations publiques que par des opérateurs privés, ne saurait être suffisante sans les institutions et opérateurs nécessaires

(4) Article 417-1 du DOC tel que complété par la loi n°53-05

(5) Article 417-2 du DOC tel que complété par la loi n°53-05

(6) Pour ce faire, la signature électronique doit être :
- propre au signataire ;
- créée par des moyens que le signataire puisse garder sous contrôle exclusif ;
- garantir la détectabilité de toute modification ultérieure avec l'acte original auquel elle se rattache ;
- produite et dûment identifiée par la personne dont elle émane et que l'acte soit établi et conservé dans des conditions de nature à en garantir l'intégrité ;
- Par un dispositif de création de signature électronique attesté par un certificat de conformité.

(7) Le prestataire agréé à cet effet, doit réunir les conditions techniques exigées par l'article 21 de la loi n°53-05 et être en mesure de conserver toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la signature électronique

(8) Barid Al Maghrib est un prestataire de services de certification électronique agrée par la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI)

pour que les règles prévues par la loi n °53-05 soient effectives. Il en est ainsi de (i) l'autorité de régulation et (II) du tiers de confiance chargé de la certification.

▪ Autorité de régulation. Conformément aux termes de l'article 15 de la loi n° 53- 05, il est institué une autorité nationale d'agrément et de surveillance de la certification électronique. L'autorité nationale est chargée d'assurer le respect par les prestataires des services de certification électronique des obligations prévues par la loi suscitée et les textes réglementaires pris pour son application.

▪ À ce jour les fonctions relevant de l'autorité nationale sont dévolues à la Direction générale de la sécurité des systèmes d'information (DGSII) relevant de l'administration de la défense nationale.

▪ Barid AL MAGHRIB. Barid AL MAGHRIB SA (Poste Maroc) est, à ce jour la seule autorité de certification chargée de délivrer les certificats numériques, de leur assigner une date de validité et de garantir l'identité de son propriétaire.

▪ Il assume à l'égard de ses abonnés et des tiers la responsabilité juridique relative aux certificats qu'il émet conformément à la loi en vigueur. À ce titre, il délivre à travers Barid eSign des certificats électroniques garantissant le lien entre l'identité d'une personne et une bi-clé de signature qui lui est associée.

▪ Les certificats délivrés, à ce jour, par l'autorité de certification sont rangés en trois catégories :

- Classe 1 : certificat logiciel P12 (9) ;
- Classe 2 : certificat sur support cryptographique (10) ;
- Classe 3 : certificat su support cryptographique évalué (11).

▪ Nonobstant la mise en place d'un cadre juridique propre à la signature électronique, dotant cette dernière de la sécurité juridique nécessaire pour qu'elle puisse être utilisée par les administrations publiques et les opérateurs privés dans le cadre de leurs prestations ou transactions, force est de constater que le succès attendu n'a pas été au rendez-vous.

▪ Le recours à l'obtention de certificats garantissant la sécurité de la signature électronique est resté résiduel.

▪ Aussi, et compte tenu des contraintes découlant de la pandémie de la Covid-19, Barid AL MAGHRIB a mis en place une procédure simplifiée pour l'obtention du certificat de classe 3, caractérisée notamment par la simplification du dossier administratif devant être présenté à l'autorité de certification pour l'obtention dudit certificat.

▪ Cependant, en l'absence d'une refonte plus approfondie des conditions d'obtention des certificats et de l'agrément de nouveaux opérateurs habilités à en délivrer, le développement du recours à la signature électronique restera limité.

(9) Il s'agit d'une classe sous format de logiciel pouvant être utilisée dans des domaines ou la force probante de la signature n'est pas requise. D'un point de vue juridique, la classe 1 donne lieu à une signature électronique simple

(10) Il s'agit de certificats établis sur des moyens physiques (cartes à puce, clé USB, …). C'est un dispositif plus sécurisé que celui de la classe 1, mais reste néanmoins considéré comme come une signature électronique simple.

(11) Le certificat classe 3 confère à la signature numérique la même valeur légale que celle des documents physiques. Elle donne lieu à une signature électronique sécurisée. Elle se présent sous forme d'une clé USB équipée d'une puce électronique contenant une clé privée et un certificat numérique. L'usage d'un certificat classe 3 est notamment requis pour toute signature électronique effectuée dans le cadre de relations avec l'administration fiscale, les établissements bancaires, entre administrations et entre entreprises.

HATIM ELKHATIB
&
AMAL AZAROUR

morocco@lexing.network

The electronic signature in Moroccan law

▪ *Social distancing measures and restrictions on the free mobility of people, following the outbreak of the Covid-19 pandemic, have led to increased use of new communication technologies, and accelerated the process of digitalization of the Moroccan administration as well as the recourse of economic operators to new information technologies to ensure the continuity of their activities remotely.*

▪ *However, this evolution can only be definitively settled insofar as the legal framework governing the conclusion of contracts by electronic means and the electronic signature allows it and that the process of establishing the legal procedures necessary for this purpose are efficient.*

The legal framework of the electronic signature in Morocco

▪ *The process of dematerialization of data started several years ago, in the wake of the development of new electronic communication technologies, remained inefficient by the lack of a legal framework ensuring the validity of contracts concluded by electronic means and the probative force of electronic signature.*

▪ *Notwithstanding the increased use of electronic data exchange and storage, as soon as the relationship between the parties was to result in the formalization of contractual commitments, recourse to the paper-based contract remained inevitable.*

▪ *Also, the will to accelerate the development of these new modes of transaction was quickly confronted with the limits of the Moroccan civil law, based on the principle of written record, provider by the DOC (1) and which did not allow the electronic signatures to produce the legal effects equivalent to the paper-based signatures.*

▪ *In the lack of an explicit legal reference to the legal value of the electronic signature, as a tool for verification of the signatory parties' identity, as well as the authentication of the contractual act's content and its attachment to the parties, its use as proof of the existence of contractual commitments was not conceivable (2).*

▪ *In this context, the Moroccan legislator adopted on November, 30th 2007, the Law n°53-05 related to the electronic exchange of legal data (3), with the aim of:*

- *Establishing the legal framework applicable to data exchanged by electronic means;*
- *Expending the equivalence of electronically exchanged documents and comprising an electronic signature to the paper-based documents;*
- *Setting the legal framework applicable to operations carried out by the certification service- providers;*
- *Establishing a national licensing and supervising authority.*

(1) Dahir des Obligations et des Contrats is the Moroccan Civil law that governs obligations and contractual commitments

(2) In this respect, in accordance with the terms of article 417 and 443 of the DOC The written proof results from an authentic instrument or from a private writing and the agreements having for purpose the establishment, the transfer, the amendment or the extinction of obligations and rights of which the values exceeds the sum of Ten Thousand (10,000) dirhams must be drafted in an authentic instrument or in private writing.

(3) Inspired on the general principles of the UNCITRAL on electronic signatures of 2001 and the Directive n°1999/93/EC on a Community framework for electronic signatures

▪ *The enactment of Law No. 53-05 resulted in the acknowledgement of the legal value of the electronic signature and its probative force through articles 417-1 (4) and 417-2 (5) of the DOC, which confirmed the equivalence of the proof established in an electronic mean to the one established in a paper based document and its probative value.*

▪ *The acceptance of the electronic signature as proof of the establishment of a contractual act is however excluded for any act relating to the family code or personal or property security interests of a civil or commercial nature.*

▪ *The reliability of the electronic signature is presumed when it has been securely established (6).*

▪ *The acknowledgment of the electronic signature and the consecration of the probative force of the electronic writing are however subjected to conditions provided by Law so as the concerned document is established and remained under conditions to guarantee the identity of the person from whom the signature or electronic document is issued as well as the integrity of the concerned legal act.*

▪ *Thus, the recognition of the electronic signature as a mean of proof depends on the use of a reliable method of identification, namely, the electronic certificate, ensuring the link with the act to which it is attached and allowing to:*

- *verify the identity of the signatory;*
- *check the integrity of the content;*
- *make the exchange of data and the signed document non-refutable;*
- *use confidential exchanges.*

▪ *As a matter of fact, the legislator has implemented security procedure for creation process of the electronic signature allowing, through hardware and/or software intended for this purpose, to identify the distinctive elements characterizing the signatory and necessary the relation of the electronic signature to its holder.*

▪ *Certification of the electronic signature can be simple or secured. The latter must meet the following conditions:*

- *be specific to the signatory;*
- *be created by means that the signatory can keep under his exclusive control;*
- *guarantee a link to the act to which it is attached so that any subsequent modification of said act is detectable.*

▪ *The electronic signature must be attested by a simple or secured compliance certificate (7).*

▪ *In order to provide the established process with the necessary legal certainty, the legislator made the right to issue electronic signature certificates subject to obtaining a license granted by the National Authority for the Licensing and supervising of Electronic Certification. To date, only Barid ALMAGHRIB (Poste du Maroc) (8) has been approved as an authority empowered to issue an electronic certificate.*

(4) Article 417-1 of the law n°53-05 related to electronic exchange of legal documents amending and completing the DOC

(5) Article 417-2 of the law n°53-05 related to electronic exchange of legal documents amending and completing the DOC

(6) For the electronic signature must be:
- specific to the signatory;
- created by means that the signatory can keep under exclusive control;
- guarantee the detectability of any subsequent modification with the original act to which the signature is related;
- produced and duly identified by the person from whom it is issued and that the document is drawn up and remained under conditions likely to guarantee its integrity;
- by an electronic signature creation device certified by a compliance certificate.

(7) The certification service provider approved for this purpose must meet the technical conditions required by article 21 of law n°53-05 and be able to keep all the information relating to the electronic certificate which may be necessary to consider the electronic signature as proof before court.

(8) Barid ALMAGHRIB (Poste du Maroc) the accredited certification service provider in Morocco, by the General Department of Information Systems Security (DGSII)

Conditions for securing the electronic signature

▪ *The establishment of legal rules providing the necessary probative force to the electronic signature so to be used on a recurring basis both by public administrations and by private operators, cannot be sufficient without the institutions and operators required to make the legal provisions effective, such for (i) the regulatory authority and (II) the entrusted third party responsible for certification.*

▪ *Regulatory authority. In accordance with the terms of article 15 of Law No. 53-05, a national authority for the licensing and supervising of electronic certification is established.*

▪ *The national authority is responsible for ensuring that the electronic certification services providers comply with the obligations laid down by the above-mentioned law and the regulatory texts adopted for its application.*

▪ *To date, the functions of national authority have been devolved to the General Department of Information Systems Security (DGSII), which is part of the National Defense Department.*

▪ *Barid AL MAGHRIB. Barid AL MAGHRIB SA (Poste Maroc) is, to date, the only certification authority responsible for issuing electronic certificates, assigning them a validity date and guaranteeing the identity of the issuer.*

▪ *It undertakes with respect to its subscribers and third parties the legal responsibility related to the certificates issued in accordance with the law in force.*

▪ *Therefore, it issues electronic certificates through Barid eSign guaranteeing the link between a person's identity and a key signature related to it.*

▪ *The certificates issued, to date, by the certification authority fall into three categories:*

- *Class 1: P12 software certificate (9);*
- *Class 2: certificate on cryptographic support (10);*
- *Class 3: certificate on evaluated cryptographic medium (11).*

▪ *Notwithstanding, the establishment of a legal framework specific to the electronic signature, providing the latter with the legal certainty necessary for it to be used by public administrations and private operators in the context of their services or transactions, it is to be noted that the expected success did not come.*

▪ *The recourse to obtaining certificates guaranteeing the security of the electronic signature remained residual.*

▪ *Also, and given the constraints arising from the Covid-19 pandemic, Barid AL MAGHRIB has implemented a simplified procedure for obtaining the class 3 certificate, characterized in particular by the simplification of application form for obtaining the aforesaid certificate.*

However, in the lack of a more thorough overhaul of the conditions for obtaining certificates and the approval of new operators empowered to issue them, the expansion of the electronic signatures use will remain limited.

(9) This is a class in software format that can be used in fields where the proof of signature is not required. From a legal point of view, class 1 gives rise to a simple electronic signature.

(10) It concerns certificates established on physical means (smart cards, USB key, etc.). It is a more secured device than that of Class 1, but nevertheless remains considered as a simple electronic signature.

(11) The class 3 certificate gives the electronic signature the same legal value as that of paper-based signature. It gives rise to a secured electronic signature.
It comes in the form of a USB key fitted with an electronic chip containing a private code and a digital certificate.
The use of a class 3 certificate is particularly required for any electronic signature made in the context of relations with the tax authorities, banking establishments, between administrations and companies.

HATIM ELKHATIB
&
AMAL AZAROUR

morocco@lexing.network

Le télétravail et la signature électronique en période Covid au Sénégal

▪ La pandémie Covid-19 aussi inattendue que prévue a paralysé l'économie mondiale. Ainsi pour ne pas envenimer la situation globale déjà catastrophique, la plupart des Etats ont trouvé dans le télétravail, la possibilité de continuer les activités économiques et éviter, autant que faire se peut, les licenciements, voire les liquidations massives d'entreprises.

▪ Au Sénégal, avec les différentes restrictions dues à la Covid-19, notamment le confinement de la population, on constate une utilisation massive des réseaux Internet fixe et mobile des opérateurs de télécommunications et une surconsommation de la bande passante due essentiellement à l'adoption du télétravail par la plupart des entreprises sénégalaises (visioconférence et appels audio entre autres). Dans ce moment particulier, où les opérateurs de télécommunications et les FAI sont mobilisés, pour garantir le fonctionnement correct des réseaux, le gouvernement, les entreprises, les banques, les compagnies d'assurance etc., se sont tous lancés dans une dynamique d'utilisation impérative et massive de la signature électronique, comme moyen privilégié d'authentification des personnes et de garantie de la confidentialité des échanges électroniques.

1-Sur le télétravail

▪ Dans les circonstances de lutte contre la Covid-19, l'employeur peut temporairement recourir au télétravail même si la législation du travail sénégalaise ne prévoit pas de dispositions particulières en la matière. En effet, l'État du Sénégal a décrété l'état d'urgence accompagné d'un couvre-feu pour limiter les déplacements et a suggéré aux administrations et aux entreprises de privilégier le télétravail. Le recours au télétravail est considéré comme un aménagement du poste de travail rendu nécessaire pour permettre la continuité de l'activité de l'administration et des entreprises et garantir la protection des agents et salariés. Le numérique fait aujourd'hui partie de notre quotidien, au travail comme dans notre vie privée. Il simplifie les échanges des courriers, favorise une meilleure communication, optimise la gestion administrative des documents.

▪ Si le télétravail présente de nombreux avantages tant pour le salarié (1), que pour les entreprises (2), il peut néanmoins présenter certains risques : isolement du salarié, augmentation de son temps de travail, difficultés à se « déconnecter » et finalement un risque d'empiètement de son activité professionnelle sur sa vie personnelle. C'est pourquoi le dispositif doit être encadré. Le marché du télétravail au Sénégal est malgré tout encore embryonnaire, et les opérateurs du secteur y ont identifié un certain nombre de freins : un retard de la législation par rapport aux pays concurrents. A titre illustratif, les sociétés de téléservices sénégalaises sont toujours soumises au droit du travail et au droit fiscal des sociétés qui ne sont pas encore adaptés au numérique.

▪ Le télétravail prolongé constitue pour les pirates informatiques une source aussi inattendue qu'inespérée pour sélectionner des points d'entrée vulnérables aux données d'entreprises les plus stratégiques. Or, le souci pour les entreprises est double : assurer une étanchéité de l'accès en dehors des entreprises à des personnes qui n'utiliseraient pas des terminaux validés d'un point de vue sécurité par le RSSI (3), et agir rapidement pour mettre en place des mesures de

REFERENCES

(1) Les avantages peuvent notamment être quantifiés ci-après : Moins de temps de transport, moins de fatigue et de stress, une capacité de concentration plus importante, une plus grande liberté et autonomie, etc.

(2) Pour les entreprises : plus grand engagement des salariés, augmentation de la productivité, amélioration de la qualité du travail, attractivité de l'entreprise, diminution de l'absentéisme, etc.

(3) Martin Sauter (2010). « 3.7.1 Gestion de la mobilité dans l'état Cell-DCH ». Du GSM au LTE : une introduction aux réseaux mobiles et au haut débit mobile (eBook) John Wiley& Sons. p. 160. ISBN 9780470978221

(4) Remote Desktop Protocol (RDP) est un protocole propriétaire développé par Microsoft qui fournit à un utilisateur une interface graphique pour se connecter à un autre ordinateur via une connexion réseau. L'utilisateur utilise à cet effet un logiciel client RDP, tandis que l'autre ordinateur doit exécuter le logiciel serveur RDP

(5) Article rédigé par Dominique Filippone, « Confinement et télétravail pire des cyberattaques est à venir » publié le 26 Mars 2020

(6) A l'Université Alioune DIOP de BAMBEY, les enseignants de l'UFR Economie, Management et Ingénierie Juridique (ECOMIJ), ont continué leurs activités administratives par l'organisation de plusieurs rencontres en ligne (Conseils d'UFR, Conseils de département, webinar en e-learning etc.)

(7) Article rédigé par Ibrahima

sécurisation adaptées en veillant par exemple à éviter d'ouvrir aux quatre vents les ports RDP (4), utilisés principalement à des fins de messagerie et de communication (5).

▪ Certaines universités privées, en traduisant les vœux du gouvernement en actes concrets, ont déjà anticipé pour terminer leur année académique, en adoptant le téléenseignement ou e-learning. Seules les universités publiques font encore de la résistance, en arguant notamment le fait que le téléenseignement risque de créer de fortes disparités entre les étudiants (qui ne sont plus physiquement dans les campus) qui sont dans des zones, pour certains, non couvertes par le réseau internet. Ce qui risque de créer un véritable problème au moment de leur évaluation finale. Il est donc intéressant de noter que pendant toute la période Covid, la plupart des UFR et leurs différentes composantes, ont continué leurs activités administratives par le télétravail via des plateformes comme ZOOM ou MEET (6).

▪ Du fait du recours au télétravail par les administrations publiques, les entreprises privées et les universités notamment, la signature de certains documents s'avère donc nécessaire. En définitive, le recours au télétravail doit présider à l'utilisation massive de la signature électronique.

2- La signature électronique

▪ En ce qui concerne l'utilisation de la signature en période Covid, force est de constater qu'au Sénégal, les systèmes informatiques des entreprises n'ont jamais été conçus pour soutenir une migration soudaine et massive du personnel du bureau vers la maison. L'opportunité pour ceux qui veulent semer le chaos, à l'aide de « rançongiciels » et de « maliciels », est très significative surtout dans les pays en développement (7). De nombreux experts en sécurité tirent ainsi la sonnette d'alarme sur les potentielles cyberattaques qui se préparent dans l'ombre pour éclater au grand jour d'ici quelques semaines, mois, voire années. Le FBI prévoit que les cyberacteurs exploiteront une utilisation accrue des environnements virtuels des agences gouvernementales, le secteur privé, les organisations privées et les particuliers à la suite de la pandémie de Covid-19. Les systèmes informatiques et les environnements virtuels fournissent des services de communication essentiels pour le télétravail et l'éducation, en plus de mener des activités régulières. Les cyberacteurs exploitent les vulnérabilités de ces systèmes pour voler des informations sensibles, cibler les particuliers et les entreprises effectuant des transactions financières et se livrer à des extorsions (8). Un Responsable de l'OMS Monsieur Flavio AGGIO (9) a déclaré sur Reuters (10) que des pirates informatiques avaient ciblé la structure avec un site web malveillant. Et la National Crime Agency du Royaume-Uni a confirmé au Wall Street Journal
« qu'elle enquêtait sur une attaque présumée de « ransomware » contre Hammersmith Medicines Research, une société de dépistage de drogues qui a effectué des essais pour le vaccin contre Ebola et d'autres traitements » (11).
« Nous avons détecté des pirates qui tentent de profiter des craintes des gens, en prétendant vendre en ligne des masques de protection par exemple, pour les inciter à révéler leurs informations de carte de crédit », a expliqué de son côté la société McAfee, « les employés ne doivent ouvrir aucune pièce jointe à un e-mail, ni cliquer sur des liens dont ils ne sont pas sûrs et les signaler immédiatement à la direction » (12).

▪ Au Sénégal, le niveau d'utilisation de la sécurité numérique reste faible par rapport aux autres pays dits développés. Cependant, l'Etat sénégalais a fait des avancées dans ce domaine avec la mise en place d'un commissariat sur la

DIEDHIOU Doctorant à l'université Alioune DIOP de BAMBEY (Sénégal), « COVID 19
et Entreprise : l'âge d'or du télétravail au Sénégal » http://www.osiris.sn/COVID-19-et-Entreprise-l-age-d-or.html

(8) Le FBI prévoit une augmentation des programmes de compromis de messagerie électronique liés à la pandémie COVID-19, Voir site Le FBI (Federal Bureau ofInvestigation)https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related- to-the-covid-19-pandemic (page consulté le 06/06/200)

(9) Flavio Agio, Responsable en chef de la sécurité de l'information de l'OMS, https://www.salutfr.net/les-pirates-informatiques-ciblent-loms-alors-que-les-cyberattaques-de-coronavirus- augmentent/

(10)(10) https://www.reuters.com/article/us-health-coronavirus-who- hack-exclusive/exclusive-elite-hackers target who as coronavirus-cyberattacks-spike-idUSKBN21A3BN

(11)(11) https://wsjoffer.com/?msclkid=378d4c5ebc4a109ea6a41285045e9df0 (page consultée le 06/06/200)

(12)(12) https://service.mcafee.com/webcenter/portal/oracle/webcenter/page/ (page consultée le 06/06/200)

(13) Loi n°2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel, (Journal officiel, 2008-05-03, n°6406)

(14) Journal officiel du Sénégal, n°6406 du Samedi 3 mai 2008

(15) Il est créé une Commission

cybercriminalité, l'adoption des lois sur la sécurité de l'information, la protection des données à caractère personnel (13), la loi sur les transactions électroniques (14). Toutes ces lois ont permis de définir un cadre juridique clair qui est un impératif pour ce secteur en constante mutation.

▪ La réponse à de telles préoccupations est précisée par la loi n° 2008-08 du 25 janvier 2008 qui vise à assurer la sécurité des transactions électroniques au Sénégal, notamment les opérations liées au commerce électronique, à la conclusion d'un contrat électronique, à l'acceptation de la signature et la preuve électroniques et, enfin, aux possibilités de transmission par voie électronique des documents ou actes administratifs. L'adoption par le gouvernement du Sénégal de la signature électronique et du chiffrement comme moyen privilégié d'authentification des personnes et de garantie de la confidentialité des échanges électroniques en est une illustration parfaite.

▪ Dans ce contexte où l'efficacité et la rapidité sont une marque de fabrique pour le monde des affaires, le télétravail, qui doit induire une résurgence de la signature électronique, devient une impérieuse nécessité pour les États et le secteur privé pour contribuer à stopper la propagation de la Covid-19. Le Sénégal semble déjà anticiper sur ces nombreuses innovations avec d'importantes initiatives entreprises par des acteurs du secteur privé en partenariat avec l'État. Grâce aux solutions développées par la Commission Nationale de Cryptologie (15), GAINDE 2000 (16), l'Agence de l'Informatique de l'État (ADIE) (17) et l'Autorité de Régulation des Télécommunications et des Postes (ARTP), en matière de sécurité numérique, notre pays est, aujourd'hui, devenu une référence dans la sous-région ouest africaine, voire toute l'Afrique. En effet, en 2004 GAINDE 2000 avait lancé ORBUS, une plateforme pour faciliter le commerce à travers le guichet unique qui a connu une première mise à niveau en 2011 avec la dématérialisation et l'introduction de la signature électronique. Cette dernière consiste à garantir l'identité du signataire et assurer l'intégrité du document signé.

▪ Dans cet ordre, le gouvernement du Sénégal, par lettre circulaire présidentielle n°0288/PR/M.SG/STCC-SSI, a proscrit l'utilisation des adresses électroniques gratuites pour la transmission des documents et correspondances officiels de l'État (18). Et par la même occasion, l'utilisation de la signature électronique et de la cryptologie par les services publics de l'État. Ainsi, par lettre circulaire présidentielle n°0328/PR, il est rappelé que toute action ou initiative relative à la Cryptologie, particulièrement la fourniture, l'importation et l'utilisation des clés des chiffrements, ainsi qu'à la Sécurité des Systèmes d'Information et à la cyber sécurité, doit être soumise à la Commission nationale de Cryptologie dont la présidence est assurée par le Ministre, Secrétaire général de la Présidence de la République, conformément à la loi 2008-41 du 20 Août 2008 sur la cryptologie au Sénégal.

▪ En tout état de cause, au Sénégal, pendant la période Covid, le recours à la signature électronique, même s'il reste une réalité, se fait timidement malgré le vœu de plusieurs entreprises du secteur privé de l'intégrer dans leur usage professionnel. En définitive, dans un contexte de recours massif au numérique et aux technologies avancées, les établissements publics et les entreprises doivent donc impérativement redoubler de vigilance avec les accès distants à leur Système Informatique. Aujourd'hui au Sénégal, même si le télétravail est une réalité qui pourrait trouver sa place dans l'entreprise, l'un des défis majeurs reste l'élargissement de la signature électronique aux autres acteurs, notamment ceux
du secteur privé marqués par la prédominance de l'informel.

nationale de cryptologie rattachée au Secrétariat général de la Présidence de la République. Voir article 4 de la Loi N° 2008-41 du 20 août 2008 sur la cryptologie a été adoptée en 2008 suivi de son décret d'application pris en 2010 (Décret no 2010-1209 relatif à la loi no 2008-41 du 20 août 2008 sur la Cryptologie au Sénégal)

(16) GAINDE 2000 est une entreprise sénégalaise leader dans le domaine du numérique, qui est spécialisée dans la facilitation du commerce, la dématérialisation pour accompagner les administrations, les entreprises et le grand public dans la modernisation des formalités www.gainde2000.com

(17) L'Agence De l'Informatique de l'État (ADIE) est une structure autonome chargée de mettre en œuvre la politique d'informatisation de l'État du Sénégal. Sa mission principale est de doter l'Administration d'un dispositif cohérent de traitement et de diffusion de l'information, répondant aux normes internationales en matière de qualité, de sécurité, de performance et de disponibilité

(18) http://www.stcc - ssi.sn/?page_id=414

MAMADOU SEYE

senegal@lexing.network

Telework and electronic signature during the Covid period in Senegal

▪ *The Covid-19 pandemic, both unexpected and expected, has crippled the global economy. To avoid inflaming the already catastrophic global situation, most countries have found in telework the possibility of continuing their economic activities and avoiding as far as possible redundancies and massive business failures.*

▪ *In Senegal, because of the various restrictions linked to Covid-19, and particularly the lockdown of the population, a massive use of fixed and mobile Internet networks and an over-consumption of bandwidth have been observed due mainly to the adoption of telework by most Senegalese companies (including video conferencing and audio calls). At this particular time, telecommunications operators and ISPs are mobilized to guarantee the proper functioning of networks and the government, businesses, banks, insurance companies, and other stakeholders have all embarked on a dynamic of imperative and massive use of electronic signatures, as the preferred means of authenticating individuals and guaranteeing the confidentiality of electronic exchanges.*

1-Telework

▪ *To fight Covid-19, employers may temporarily use telework even if Senegalese labour legislation does not contain any specific provision on telework. Senegal has declared a state of emergency accompanied by a curfew to limit travel and encouraged government agencies and companies to give priority to telework. The use of telework is considered to be a working arrangement necessary to allow the continuity of the economic activity and guarantee the protection of agents and employees. Today, digital technology is part of our daily lives, both at work and at home. It simplifies the exchange of mail, promotes better communication and streamlines the administrative management of documents.*

▪ *While telework has many advantages for both the employee (1) and the company (2), it can nevertheless present certain risks: isolation of employees, increase in their working time, difficulties in "disconnecting" from work life and therefore a risk of work-life imbalance. That is why telework needs to be regulated. The telework market in Senegal is still in its infancy, and operators in the sector have already identified a number of obstacles caused by a delay in legislation compared to other countries. Senegalese teleservice companies are required to comply with labour laws and corporate tax laws, which are still not adapted to digital technology.*

▪ *Moreover, prolonged telework provides hackers with an unexpected and unhoped-for source for selecting entry points vulnerable to the most strategic corporate data. The concern for companies is twofold: to ensure that people who do not use terminals whose security has been validated by the CISO do not access information systems (3), and to quickly put in place appropriate security measures*

REFERENCES

(1) Advantages for employees include less travel time, less fatigue and stress, greater ability to concentrate, greater freedom and autonomy.

(2) Advantages for companies include: greater employee commitment, increased productivity, improved quality of work, attractiveness of the company, reduced absenteeism.

(3) Martin Sauter (2010). "3.7.1 Gestion de la mobilité dans l'état Cell-DCH". Du GSM au LTE : une introduction aux réseaux mobiles et au haut débit mobile (eBook) John Wiley& Sons. p. 160. ISBN 9780470978221

(4) Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

(5) Article drafted by Dominique Filippone, "Confinement et télétravail pire des cyberattaques est à venir" published on 26 March 2020

(6) At the University Alioune DIOP de BAMBEY, the teachers of the Economy, Management and Legal Engineering (ECOMIJ) unit continued their administrative activities by organising several online meetings (councils, department Councils, webinar in e-learning...).

(7) Article drafted by Ibrahima DIEDHIOU (PhD student at University Alioune DIOP de BAMBEY, Senegal), "COVID 19 et Entreprise : l'âge d'or du

by ensuring, for example, that the RDP ports (4) (which are used mainly for messaging and communication purposes) are not unprotected (5).

▪ *Some private universities, applying the recommendations of the government, have adopted distance learning or e-learning until the end of their academic year. Only public universities are still resisting, arguing in particular that distance learning risks creating strong disparities between students (who are no longer physically on campus) as some of them lived in areas not covered by the Internet. This may create a real problem when students will be subject to their final evaluation. It is interesting to note that throughout the Covid period, most of the university research and training units continued their administrative activities through telework via platforms such as ZOOM or MEET(6).*

▪ *The large number of people from public agencies, private companies and universities working from home makes it necessary to electronically sign certain documents. Telework will ultimately lead to the widespread use of electronic signatures.*

2- Electronic signature

▪ *In Senegal, the computer systems of most companies were never designed to support a sudden and massive migration of staff from office to the home. Such situation opens up opportunities for those who want to cause chaos, with the help of ransomware and malware, especially in developing countries (7). Many security experts are thus sounding the alarm about the potential cyberattacks, which are being prepared in the shadows and are set to erupt in the coming weeks, months or even years. The FBI anticipates that cyber actors will take advantage of Covid-19 pandemic to exploit increased use of virtual environments by government agencies, the private sector, private organizations and individuals. Computer systems and virtual environments provide essential communication services for telework and education, in addition to conducting regular business. Cyber actors exploit vulnerabilities in these systems to steal sensitive information, target individuals and businesses performing financial transactions, and engage in extortion (8). A World Health Organization official Mr Flavio AGGIO (9) said to Reuters (10) that hackers had targeted the WHO with a malicious website mimicking its internal email system. And the U.K. National Crime Agency confirmed to the Wall Street Journal "*that it is investigating an alleged ransomware attack against Hammersmith Medicines Research, a drug-testing company that has carried out trials for the Ebola vaccine and other treatments*" (11) "*We've seen hackers attempt to take advantage of people's fears by pretending to sell face masks online to trick unsuspecting people into giving away their credit card details.*" McAfee said. "*Do not open any email attachments or click on any links that seem suspicious *(12)."*

▪ *In Senegal, digital security remains low compared to other so-called developed countries. However, the Senegalese state has made progress in this area and established a commissioner's cybercrime office, the adoption of laws on information security, protection of personal data (13), and electronic transactions (14). All these laws have made it possible to define a clear legal framework, which is essential for this constantly changing sector.*

télétravail au Sénégal" http://www.osiris.sn/COVID - 19-et-Entreprise-l-age-d-or.html

(8) FBI anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic. See Federal Bureau of Investigation (FBI) site. https://www.fbi.gov/news/pre ssrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic (page consulted on 06/06/200)

(9) Flavio Agio, Chief Information Security Officer, WHO, https://www.salutfr.net/les-pirates-informatiques-ciblent-loms-alors-que-les-cyberattaques-de-coronavirus- augmentent/

(10) https://www.reuters.com/artic le/us-health-coronavirus-who- hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

(11) https://wsjoffer.com/?msclkid=378d4c5ebc4a109ea6a41285045e9df0 (page consulted on 06/06/200)

(12) https://service.mcafee.com/webcenter/portal/oracle/webcenter/page/ (page consulted on 06/06/200)

(13) Loi n°2008-12 du 25 janvier 2008 portant sur la protection des données à caractère personnel, (Official Journal, 2008-05-03, No. 6406)

(14) Senegal Official Journal, No. 6406 of Saturday 3 May 2008

(15) A National Cryptology Commission attached to the General Secretariat of the Presidency of the Republic has

▪ *The Law No. 2008-08 of 25 January 2008 aims to ensure the security of electronic transactions in Senegal, including operations related to e-commerce, the conclusion of an electronic contract, the acceptance of electronic signature and proof and the possibility of transmitting administrative documents or acts electronically. The adoption by the Senegalese government of electronic signature and encryption as the preferred means of authenticating individuals and guaranteeing the confidentiality of electronic exchanges is a perfect illustration of this.*

▪ *In a context where efficiency and fastness are unavoidable for a competitive business world, telework, which should lead to a resurgence of electronic signature, is becoming a must for States and businesses to help stop the spread of Covid-19. Senegalese stakeholders have already planned to set up measures to anticipate these numerous innovations with important initiatives undertaken by the private sector actors in partnership with the Government. Thanks to the IT solutions developed by the National Cryptology Commission (15), GAINDE 2000 (16), the state information technology agency (ADIE) (17) and the Telecommunications and Postal Regulatory Authority (ARTP) regarding digital security, Senegal has become a remarkable reference in Africa in general and in the West African subregion in particular. In 2004, GAINDE 2000 launched ORBUS, a platform to designed to facilitate trade through a Single Window system that has experienced first upgrade in 2011 with the dematerialization and the introduction of the E-signature. The latter consists in verifying the signatory's identity and the file's integrity.*

▪ *In the same vein, by Presidential Circular Letter No 0288/PR/M.SG/STCC-SSI, the government of Senegal prohibited the use of free email addresses for the transmission of official state documents and correspondence (18). And at the same time, the use of electronic signatures and cryptology by the State's public services. Thus, by presidential circular letter n°0328/PR, it is recalled that any action or initiative relating to cryptology, particularly the supply, importation and use of encryption keys, as well as to Information systems security and cyber security, must be submitted to the National Cryptology Commission chaired by the Minister, Secretary General of the Presidency of the Republic, in accordance with Law 2008-41 of 20 August 2008 on cryptology in Senegal.*

▪ *In any event, the use of electronic signatures in Senegal during the Covid-19 period remains low despite the desire of several private sector companies to integrate it into their professional use. In a context where digital and advanced technologies are massively used, public and private originations must carefully monitor any remote access to their IT systems. Today, in Senegal, even if telework could find its place in companies, one of the major challenges remains the extension of electronic signature to other actors, especially those in the private sector marked by the predominance of the informal sector.*

been created. See article 4 of Law No. 2008-41 of 20 August 2008 adopted in 2008, followed by its implementing decree issued in 2010 (Decree No. 2010-1209 on Law No. 2008-41 of 20 August 2008 on Cryptology in Senegal).

(16) GAINDE 2000 is a leading Senegalese company in the field of digital technology, specialising in trade facilitation and digital transformation to support administrations, businesses and the general public in modernising formalities www.gainde2000.com

(17) The Agence De l'Informatique de l'Etat (ADIE) is an autonomous structure responsible for implementing the computerization policy of the State of Senegal. Its main mission is to provide the administration with a coherent system for processing and disseminating information that meets international standards of quality, security, performance and availability.

(18) http://www.stcc-ssi.sn/?page_id=414

MAMADOU SEYE

senegal@lexing.network

LEXING NETWORK

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons	John Giles	+27 (0) 21 300 1070	south-africa@lexing.network
Allemagne *Germany*	Beiten Burkhardt	Andreas Lober	+49 69 756095-0	germany@lexing.network
Australie *Australia*	Gadens	Dudley Kneller	+61 438 363 443	australia@lexing.network
Belgique *Belgium*	Lexing Belgium	Jean-François Henrotte	+32 4 229 20 10	belgium@lexing.network
Canada *Canada*	Langlois avocats, S.E.N.C.R.L.	Jean-François De Rico	+1 (418) 650 7000	canada@lexing.network
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	china@lexing.network
Costa Rica *Costa Rica*	Lexing Costa Rica	Gabriel Lizama	+506 2253-1726	costa-rica@lexing.network
Côte d'Ivoire *Ivory Coast*	Imboua Kouao Tella & Associés	Annick Imboua-Niava	+ 225 22 44 74 00	ic@lexing.network
Espagne *Spain*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	spain@lexing.network
États-Unis *USA*	DataMinding Legal Services	Françoise Gilbert	+1 650-804-1235	usa@lexing.network
France *France*	Alain Bensoussan-Avocats Lexing	Alain Bensoussan	+33 1 82 73 05 05	france@lexing.network
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	greece@lexing.network
Hongrie *Hungary*	OPL - Orbán & Perlaki	Miklos Orban	+36 1 244 8377	hungary@lexing.network
Inde *India*	Poovayya and Co	Siddhartha George	+91 80 4115 6777	india@lexing.network
Israël *Israel*	Appelfeld & Co	Ilanit Appelfeld	+ 972 3 60 98 099	israel@lexing.network
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	italy@lexing.network
Japon *Japan*	Hayabusa Asuka Law Office	Koki Tada	+81 3 3595 7070	japan@lexing.network
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	lebanon@lexing.network
Luxembourg *Luxembourg*	Emmanuelle Ragot	Emmanuelle Ragot	:(+352) 661 84 42 50	luxembourg@lexing.network
Maroc *Morocco*	Elkhatib Lawfirm	Hatim Elkhatib	+212 5 39 94 05 25	morocco@lexing.network
Mexique *Mexico*	Carpio, Ochoa & Martínez Abogados	Enrique Ochoa De Gonzälez Argüelles	+ 52 55 25 91 1070	mexico@lexing.network
Norvège *Norway*	Advokatfirmaet Føyen Torkildsen AS	Arve Føyen	+47 21 93 10 00	norway@lexing.network
Nouvelle-Calédonie *New Caledonia*	Cabinet Franck Royanez	Franck Royanez	+ 687 24 24 48	nc@lexing.network
République tchèque *Czech Republic*	Rowan Legal	Josef Donát Michal Nulíček	+420 224 216 212	czechrepublic@lexing.network
Royaume-Uni *United Kingdom*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	uk@lexing.network
Sénégal *Senegal*	SCP Faye & Diallo	Mamadou Seye	:(+221) 33 823 60 60	senegal@lexing.network
Slovaquie *Slovakia*	Rowan Legal	Josef Donát Michal Nulíček	+420 224 216 212	slovakia@lexing.network
Suisse *Switzerland*	Sébastien Fanti	Sébastien Fanti	+ 41 (0) 27 322 15 15	switzerland@lexing.network

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan. Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier
Diffusée uniquement par voie électronique – gratuit– ISSN 1634-0701
Abonnement à partir du site : https://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-debat/