CHAPTER 17 **DIGITAL**

DIGITAL TRANSFORMATION AND SUSTAINABLE DEVELOPMENT – INDUSTRY 4.0

Vietnam ranked 42nd out of 129 countries and economies surveyed in the World Intellectual Property Organisation's "Global Innovation Index" (GCI) in 2019.[1] On top of this, in the World Economic Forum's "Global Competitiveness Index" (GCI) Vietnam was the most-improved of all 141 countries in the report, ranking 67th in 2019.[2] Vietnam's digital economy has increased by more than 40 per cent per year and is considered a leader in South-East Asia.[3] Meanwhile, Hanoi and Ho Chi Minh City are among the ten most dynamic cities in the world.[4]

Looking towards the decade 2020-2030, the Government of Vietnam is accelerating its efforts, together with other countries, to achieve the Sustainable Development Goals in 2030 Agenda based on the country's impressive economic growth.[5] To this end, the Ministry of Planning and Investment (MPI) formulated a Draft in July 2019 called the "National Strategy for the Fourth Industrial Network until 2030".

The potential of Industry 4.0 for public and private companies in Vietnam is enormous. This not only applies to the optimisation of manufacturing and administrative processes but also to the development of new business models. Critical success factors for this challenging target include: a common strategy of politics and economy; competence building; education and training; the involvement of employees in the change process; powerful scalable infrastructures (wireless and wired); cyber security; network with stakeholders in the regions; combined forces; the promotion of start-ups; growth and financing; as well as the contributions of national and international market participants, the public sector and organisations.

Industry 4.0 could bring significant benefits through different channels. Over the next 10 years, it is estimated that the GDP of Vietnam will increase from US$28.5 billion to US$62.1 billion based on the degree of Industry 4.0 implementation in companies. Industry 4.0 will also change the structure of work in the economy. Estimates assume that, by 2030, both the number of jobs and labour productivity will increase significantly.[6]

In this chapter, the EuroCham Digital Sector Committee[7] provides more details on three topics which we suggest the Government to prioritise. These include:

- Human capital and education
- E-signature
- The Cyber Security Law.

These topics were chosen by our Digital Sector Committee members through discussion and a careful process of deliberation.

We hope that local partners, the Government and relevant authorities will consider our recommendations based

1 "Global Innovation Index", *World Intellectual Property Organization*, 2019, available at <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2019.pdf?, last accessed on 8 December 2019.
2 The Global Competitiveness Report 2019", *World Economic Forum*, 2019, available at <http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf>, last accessed on 8 December 2019.
3 "E-Economy SEA 2019", *Google Blog*, 2019, <https://www.blog.google/documents/47/SEA_Internet_Economy_Report_2019.pdf>, last accessed on 8 December 2019.
4 "City Momentum Index 2019", JLL, 2019, available at <https://www.jll.co.uk/en/trends-and-insights/research/city-momentum-index-2019>, last accessed on 8 December 2019.
5 "PM chairs National Conference for Sustainable Development 2019", *Vietnam Economic Times*, 13/09/2019, available at: <https://www.vneconomictimes.com/article/vietnam-today/pm-chairs-national-conference-on-sustainable-development-2019>, last accessed on 8 December 2019.
6 "Opening Vietnam up to Industry 4.0", *Vietnam Investment Review,* 08/05/2019, available at <https://www.vir.com.vn/opening-vietnam-up-to-industry-40- 67590.html>, last accessed on 8 December 2019.
7 On 13 March 2020, EuroCham Information and Communication Technology Sector Committee has changed its name to the Digital Sector Committee

on the international experiences of our members and best practice in Europe and treat them as a useful resource to help achieve their development goals for Vietnam. We would welcome the opportunity to discuss these issues further and in detail with relevant Ministries.

I. HUMAN CAPITAL AND EDUCATION IN THE DIGITAL AGE

Relevant authorities: Ministry of Information and Communication (MIC), Ministry of Education and Training (MOET), Ministry of Labour, Invalids and Social Affairs (MOLISA)

Issue description

Rising skills can be used as a signpost for how an economy is transforming or innovating. While rising skills are unsurprisingly largely dominated by technical skills, soft skills are also growing in prominence. This is because tech is breaking out of its silos and soft skills such as creativity, problem solving, and critical thinking are in demand to expand the application of new technology.

Today, most company managers including those in public services, hiring managers and recruiters find themselves confronted with this human resource crisis. In fact, by 2020, APAC will face a labour shortage of 12.3 million workers at an annual opportunity cost of US$4.2 trillion.[8] At the heart of this crunch lies skills instability.

According to a World Economic Forum report on the "Future of Jobs", by 2022, the skills required to perform most jobs will have shifted significantly. Globally, an average of 42 per cent of the core skills required to perform a job will change between 2018 and 2022.[9]

APAC's talent crunch is exacerbated because the region exports more talent than it imports, resulting in the lack of availability of skills and skills instability.

Potential Gains/Concerns for Vietnam

Speed and agility are essential in a digital world and in this transformation process to Industry 4.0. The future of work is about creating a new relationship between technology and talent that transforms existing work and business practices. Automation and digitisation in the workplace, machinery, robots, artificial intelligence and "smart" information technology are increasing worldwide and offer great opportunities for jobs in Vietnam. This technology has the potential to free Vietnamese workers from lower value-added tasks and give them the opportunity to accept potentially higher-quality jobs.

The increasing degree of digitisation in the Vietnamese economy and public services generally requires more expertise. This applies equally to academic and vocational education. Schools also need to keep pace with technological progress in terms of their staff and equipment. In addition, the prerequisites must be created so that the skills are taught in schools.

One of the key objectives included in the Government's reform plan for middle and higher education is to improve the teaching quality of academics employed in higher education. A goal set by the government was that all academics will be at least masters, and preferably doctoral-qualified by 2020.

However, many vocational education college and university courses do not feature work-based learning opportunities or industry placements, so omit valuable, actual practical experience from students' learning. Therefore, most graduates have little or no practical experience in business, in enterprises or in an international environment. Most importantly, in the IT sector, the knowledge imparted cannot meet the requirements of the digital economy and cannot support this process of digital transformation 4.0 efficiently.

The biggest challenge for academics resides in the need for real change to occur in the teaching-learning

8 "The Future of Work.", *Korn Ferry*, 2018, available at <https://futureofwork.kornferry.com/>, last accessed on 8 December, 2019.

9 The Future of Jobs Report 2018", *World Economic Forum*, 17 September 2018 available at <https://www.weforum.org/reports/the-future-of-jobs-report-2018>, last accessed on 8 December 2019.

approach used, designing curriculums that include activities to provide opportunities for learners to understand real-world, up-to-date problems.

Recommendations

In order to address the above-mentioned issues, we would like to make the following specific recommendations for different education sectors:

- Education organisations and their lecturers should intensify and improve their cooperation with national and international enterprises. They should cooperate to provide real world experience training and curriculum development;
- Key universities could support universities in the regions through regular exchange of knowledge and experiences to, in a sense, "train the trainers";
- A longer mandatory internship at IT companies or IT departments in medium and large enterprises should be ensured;
- Programs should reflect the fact that there are around 20 specialised IT occupations. Moreover, students need to understand, choose and study one or more specialised IT occupation program from their second year, which will develop their professional competence;
- Vocational colleges could also improve if they combine part-time study and apprenticeship. The successful completion leads to certification in a particular trade or field of work[10] ; and
- Politicians, together with companies, associations and trade unions, are called upon to counter any fears and to promote acceptance of capacity building.

II. E-SIGNATURE

Relevant authorities: the Government, The National Electronic Authentication Centre (NEAC)

Electronic signatures have been recognised by law in Vietnam since 2005 and can now be applied for the majority of general business transactions. We acknowledge with appreciation recent efforts of the Government and the Ministry of Information and Communication in promoting the use of electronic signatures in the future.[11] However, several difficulties still remain in their adoption resulting in the business community's reluctance to use electronic signatures in general business transactions.

Issue description

According to Article 9 of Decree 130/2018/ND-CP[12], it is understood that the valid use of electronic signatures is closely linked to the requirement of a digital certificate: Electronic signatures are considered secured electronic signatures if they are created during the valid period of digital certificates and inspected by the public key recorded on such valid digital certificates; and are created by using the private key corresponding to public key recorded on digital certificates. These digital certificates are granted by public certification authorities who have a license granted by the Ministry of Information and Communications, such as VNPT, Nacencomm, BKAV, Viettel, FPT, etc.

However, the electronic signature overseen by the Government, known as a Qualified Electronic Signature (QES), is only one distinct type of electronic signature. Meanwhile, from applicable laws, we understand that any type of electronic signature could be used:

10 For example, Dual vocational education of AHK Vietnam with the brand AKH Academy, AHK HCMC, Deutsches Haus.

11 "State organisations to promote use of digital signatures", *Vietnam News*, 13 October 2019. Available at <http://vietnamnews.vn/society/536830/state-organisations-to-promote-use-of-digital-signatures.html#VZQhguObG2oUhZKU.99> last accessed on 8 December 2019.

12 Decree 130/2018/ND-CP dated September 27, 2018 of the Government guiding the Law on e-transactions of digital signatures and digital signature authentication.

- Article 124.1 of the Civil Code 2005, replaced by Article 119 of the Civil Code 2015, regulates that civil transactions by way of electronic means in the form of data messages prescribed in the law on electronic transactions shall be deemed to be written civil transactions.
- Article 14.1 under the Law on E-transaction[13] further regulates that a data message cannot be disclaimed in terms of its validity as evidence for the sole reason that it is a data message.

The lack of comprehensive regulations on the adoption of digital signatures has led to confusion and reluctance from both foreign and local enterprises in applying solutions other than qualified electronic signatures with a digital certificate and token. Multiple other electronic signature solutions[14] are available on the market. However, it is not clear whether they are compliant with prevailing regulations and standards,[15] nor if they are legal or recognised for either local or global business transactions.

The European business community has taken note of many cases when local companies are not sure about the application of electronic signatures and how to check the validity of an electronically signed document, leading to delayed administrative approval. Our member companies have encountered cases when business contracts have been signed electronically between an overseas company and a local Vietnamese company using other solutions, but the local bank in Vietnam has denied the validity of the contract as a justification to approve the related inbound or outbound wire transactions. On the other hand, this same bank accepts the un-notarised, scanned hand-signed business contract by email as valid document despite the fact that the scanned contract could have been falsified more easily. Not until weeks later, after many exchanges between the local company and the local bank, did the local bank accept electronically signed contract as valid.

Recommendations

Thanks to Circular 16/2019/TT-BTTTT[16] taking effect from 1 April, 2020, clarification of compulsory standards has been provided for digital signatures and digital signature authentication services according to a digital model on mobile devices and remote digital signatures. It also clarifies the relevant Government authorities, namely The Ministry of Information and Communications, the Department of Science and Technology and the National Electronic Authentication Centre (NEAC).

However, we would appreciate support from NEAC on evaluating non-QES electronic signature solutions with both local and international solutions and providing a non-exhaustive list of non-QES solutions that have met the compulsory standards.

Eurocham remains at the disposal of the Government and relevant authorities if any further details are needed.

III. CYBER SECURITY LAW AND THE DRAFT DECREE ON CYBER SECURITY

Relevant authorities: Ministry of Information and Communication (MIC), Ministry of Public Security (MPS)

Issue description

In 2018, the GDPR[17] came into force in Europe to protect the personal information of individuals, creating a framework to govern the treatment and diffusion of individuals' data.

13 Article 4.1 of the Law on E-transactions No. 51/2005/QH11: "A data message cannot be disclaimed in terms of its validity as evidence for the sole reason that it is a data message."
14 For example, DocuSign, PandaDoc, SignRequest, ZohoSign,…
15 For example, the National standard TCVB 7635:2007 on Cryptography technique - Digital signature.
16 Circular 16/2019/TT-BTTTT dated 5 December, 2019 of Ministry of Information and Communication on the list of compulsory standards for digital signatures and digital signature authentication services according to digital model on mobile devices and remote digital signatures.
17 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

On 12th June 2018, the National Assembly of Vietnam adopted the Cyber Security Law (CSL) regulating activities on protection of national security and social orders on Vietnamese cyberspace. The CSL came into force on the 1st of January 2019. Upon its effectiveness, enterprises providing services on Vietnamese cyberspace must fulfil various cybersecurity obligations. Article 1: Scope of the CSL aims to define and set up measures and conditions for cybersecurity at the individual scale, the corporate scale and the national scale:

Individual scale: Personal data of employees or customers of companies mentioned in Article 26 of the CSL needs to be stored in Vietnamese territory. Furthermore, such companies are also required to have a commercial representative in Vietnam[18];

Corporate Scale: Enterprises providing services on the telecom network, internet and value-added services in cyberspace in Vietnam must apply the CSL;

National scale: All provisions under the CSL aim to protect and enhance the cyber sovereignty and cyber security of Vietnam and thus protect cyberspace from cyber-attack, cyber-terrorism, cyber-espionage or cyber-crime.

It is also mentioned in Chapter V, Article 26 that the CSL concerns any domestic and foreign companies involved in cyberspace: Telecommunication services, data storage and sharing in cyberspace; providing national or international domain names for service users in Vietnam; e-commerce; online payment; intermediary payment services; transport connection services via cyberspace; social networks and social media; online games; and other information provision, management, operation in cyberspace under the forms of text messages, voice calls, video calls, emails, online chats.

Non-exhaustive key rules include that companies must:

- Publish all information demanded by the State-authority in case of doubt of cyberattack;
- Set-up appropriate mechanisms for personal data verification;
- Prevent the sharing or deleting of information containing any illegal content propaganda against the Socialist Republic of Vietnam;
- Promptly suspend the production of digital devices and the provision of cyber services and applications in case of disrupted cybersecurity;
- Have an information administrator ensuring the application of the CSL; and
- Corporates which engage in cyber space and in activities involving data collecting and processing should not ignore warnings and written requests from the relevant authorities of Vietnam relating to cybersecurity.

Also, the data localisation and local office requirement provisions, stipulated under Article 24.3 of the CSL, continues to cause concerns among EU-based companies in Vietnam. We acknowledge the clear scope of enterprises subject to the data localisation and local office requirements, the types of data to be stored in Vietnam and the grace period for such requirements stipulated in the revised draft Decree guiding the Law on Cyber Security (Draft Decree). We would like to acknowledge, as well, the extent to which sensitive data can be duplicated in the headquarters of an enterprise in their own country for technical and/or legal concerns, as long as copies remain on Vietnamese soil.

Potential gains/concerns for Vietnam

The CSL establishes a comprehensive legal framework in Vietnam for cyber sovereignty and cybersecurity. Knowing of the increase in cybercrime in South-East Asia[19], the establishment of a CSL plan in Vietnam indeed seems compulsory to protect companies as well as the Government against cyber-attacks and cyber-crimes. On

18 According to the draft Decree elaborating on a number of Articles of the Law on Cybersecurity, version of 2 November 2019 from the Department for Prevention and Combat against High-tech Crimes (Draft Decree), as long as domestic and foreign enterprises comply with the Law on Cybersecurity, and do not ignore warnings and written requests from the relevant authorities of Vietnam relating to cybersecurity, such enterprises shall not be subject to these requirements.

19 "Southeast Asia's cybersecurity an emerging concern", *The Asean Post*, 20 May 2018, available at <https://theaseanpost.com/article/southeast-asias-cybersecurity-emerging-concern>, last accessed on 8 December 2019.

that matter, one of our concerns is the liability of foreign companies whose data could be considered compromising from a CSL perspective. Although cooperation shall be provided when requested, one's responsibility should hardly be at stake upon assessing the compromising character of one's data.

Where Vietnam's CSL focuses on the regulation of the national cyber space, the European GDPR focuses on the individual data regulation of EU citizens. Therefore, it seems that for most European companies doing business in Vietnam, the Vietnam CSL seems not to be in conflict with European GDPR.

Recommendations

We would like to make the following specific recommendations:

- Set up a web portal, also accessible for foreign companies, with the necessary resources including practical guidance, training leaflets for the staff, a forum, templates for the conformity files, basic consulting, and a pool of certified companies that could support the implementation of CSL;
- Consider the gap in local expertise when compared with foreign cyber security solution leaders. Involve foreign external companies with strong expertise to ensure the feasibility of such a project to be rolled-out following the technical requirements;
- Set a grace period of reasonable length for enterprises subject to data localisation and local office requirements provision to complete the data storage and establishment of branches or representative offices in Vietnam
- The Law on Cyber Security provides an opportunity for public and private organisations to work together without losing the knowledge or freedom that the Internet has brought us. The legal implications should not lead to an undue increase in the cost of doing business or limit the easy use of the Internet. We recommend the Government works with innovators to provide standards-based cyber security capabilities which should balance both national security and business needs. This will accelerate the adoption of security technologies across industries and provide guidelines to establish hardware and software infrastructure with practical ways to implement cost-effective cyber security solutions. Moreover, a Single Data Privacy Law which protects end-consumers' private information stored on their systems should also be developed in the near future;
- Following the positive progression of the EVFTA, we would like to see the implementation of the new Law on Cyber Security brought in line with the commitments and spirit of the EVFTA to ensure the stability of the national economy as well as bilateral trade. Regarding the transparency of the adoption process, it is important to enable a public and transparent re-transmission of authorities, especially on such an important topic for the public and for the privacy of citizens. EuroCham also looks forward to commenting and working on the further draft regulations guiding the implementation of the Law on Cyber Security to ensure its consistent implementation though the guiding Decrees and other upcoming regulations; and
- Complete the legal framework and issue detailed regulations on cyber security alongside ensuring transparency and awareness while reaching out for the opinions of the business communities and technical experts.

ACKNOWLEDGEMENTS

EuroCham Digital Sector Committee