DIGITAL SOVEREIGNTY IN SALES

Mostapha Bouyrakhen
University of Library Studies and Information Technologies

Abstract: In recent years, “digital sovereignty” has not only become a political motif, but has also arrived in the business world. It is always about people and companies being able to act and decide for themselves in the digital space. The focus is on aspects such as data sovereignty, data protection, security and trustworthy infrastructures.

Keywords: Digital, Data, Sales, Europe, Sovereignty.

Introduction

The virtual footprint of companies has increased as the corporate world is changing and thus demanding better and innovative techniques to stay competitive. Digital sovereignty refers to the ability to have control over the business”s data, software, and hardware, and in an organizational context, it means that the organization has the access to delete, store, use, and manage data anytime it wants without any hindrance. Companies wish to become digitally sovereign in sales by deciding how sales data can be utilized and by whom. There are various degrees of digital sovereignty on a continuum of low to high levels of dependency along with categories. This paper will highlight the digital sovereignty in B2B sales along with EU and German perspectives in creating their digital platforms to maintain digital sovereignty.

Digital Sovereignty

The concept of digital sovereignty came about in the 2000s with its early definition 'it is the control of destiny and present as manifested by technology usage and computer networks’. Not only are the companies and organizations making the quest for digital sovereignty but government and individuals are as the influence of GAFA (Google, Apple, Facebook, and Amazon) has increased [1]. Digital sovereignty comprises various categories and options in terms of data, interfaces, source code, hardware, diversity, skills, and jurisdiction; within these categories, a business strives to have high control. In the B2B sales, the GAFA has waived the rights of the buyers as their data is no more secure but clients continue to purchase without understanding the repercussions of their actions for personal data. Digital sovereignty intends to make businesses realize that companies need to change their patterns and generate authentic automation as well as to

adapt their services for regaining control over data and the trust of consumers.

More ethical and virtuous practices have been adopted by businesses nowadays to prove their social responsibility. Only two-thirds of 15% of French people have trust in big data while the test assumes that the companies who offer tailored services use big data to track consumer's data[1] thus it is important that digital sovereignty is maintained to meet the new requirements of transparency, security, and confidentiality.

European Digital Sovereignty

In the European states, there is a call for strategic digital autonomy and the German Government has announced the establishment of digital sovereignty as the leitmotif of European digital policy[2]. The US Cloud Act impedes digital sovereignty as it allowed US agencies to transfer UK's data and the German federal government still purchased Microsoft products. Hence the German government is planning for digitally sovereign private cloud solutions along with hybrid cloud infrastructure for the private sector. The Gaia-X project has a goal of creating a trustworthy European data infrastructure and an open-source ecosystem solution along with access to a Single Market to protect intellectual property[3]. In terms of healthcare data policy, 90% of EU citizens expect that their health-related data is secure and not shared with anyone. Therefore, the German Presidency specifically and the EU generally, seeks to engage in discussions on cyberspace and strengthening capacities for malware cyber activities. Innovations like Artificial intelligence, cloud computing, 5G, and the Internet of things (IoT) have increased in the last decade with an expectation of the digital market to reach €2.2 trillion by 2025 in the EU[3]. Therefore, Europe has plans to facilitate data collection, data sharing, and data processing especially in B2B and G2C domains. Programs like Next Horizon Europe, Digital Europe, and Public-Private Partnerships (PPP) are initiated by the EU to keep pace with digital sovereignty and transformation [2].

Digital Sovereignty in B2B Sales

B2B sales is an acronym for business-to-business sales and refer to sales of products or services to other businesses. The COVID-19 pandemic has hiked online sales with consumers approaching online platforms for purchasing and buying essentials. According to McKinsey Report (2020)[4], more than 90% B2Bs have transformed into a virtual sales model with Germany facing 40% of the B2B field sales via digital conferences. The evolutionary shift from traditional to online shopping demands the digital sovereignty of consumer data with data protection. In the B2B sales, a layer of information and communication technologies are involved especially in

the manufacturing sector, so the dependencies on such cloud services demand protection as in the future, these B2B services will provide value to the economy[5]. Each company must have freedom of choice in leveraging information and the ability to offer their cloud services; they can easily evaluate the sales data and know which investors turned best.

The deployment of Europe's submarine cables and satellite-based communications can not only help improve digital speed but also allow European companies to develop their online networks, hence ensuring cyber-security and data security[6]. The data driven B2B selling companies have the potential to earn valuable revenue due to which the European Commission's 2030 vision is to provide 90% of European SMEs with big data and Artificial intelligence platforms along with 75% of big enterprises with big data and personal cloud computing services[7]. The World Wide Web has helped businesses in attracting consumers through effective marketing and most businesses are taking turns opening their sites with web adoption rate being skyrocketed. Soon, the internet became a hacker playground that disturbed the online market supremacy which destroyed the vision and sovereignty of businesses. Strong speculation was on the rise with anti-sales movements and theft of information that was related to B2B customers [3].

Digital sovereignty in business and sales implies that the national and state policies are well-grounded to protect the digital industry. One of the axes of digital sovereignty includes the removal of inequality which implies that the technological divide must be reduced by investing in the digital skills of people. 85% of the jobs in 2030 do not even exist yet which means that the labor force needs training along with their upskilling and reskilling so that no one is left behind[8]. On a broader scale, the companies need the best digital infrastructure and it is their right to utilize every digital channel disregarding their size or scale. The government should ensure that each firm or organization is provided with green transition technologies, AI, sustainable digitalization tools, and supporting key sectors which is part of digital sovereignty too [4]. Fiscal incentives and digital transformation support by countries help companies in building long-term plans with the usage of modern tools to increase B2B sales. The sales in B2B can only increase if the companies have their online platforms with a fair exchange of data and control over usage so that records can be tracked.

The B2B sellers have various concerns about digital sovereignty and these include economic, strategic, and national security concerns. Strategic concerns mean that on a mass level, the data is leaked to other countries which becomes a hindrance in decision making a secondly economic concerns pertain to the fact that customer or firm-level data does not remain confidential on the World Wide Web as many sites like Facebook and

Google use that data for marketing purposes even without the consent of the company [5]. Facebook is recently accused of leaking the personal information of 533 million Facebook users to sites like Twitter and Google which eventually resulted in public outrage as the people were concerned that their address, phone numbers, and date of birth, are used without permission[9]. Thirdly, there are political concerns among states that digital sovereignty for every individual must be maintained as already been discussed by the EU initiatives. Lastly, national security concerns also demand digital sovereignty as identity theft, fraud, coercion, hacking, and manipulation can harm the integrity of the users and create chaos.

The introduction of technical features in a business model demands effective encryption and user-friendly approaches such as increasing media literacy which strengthens the competency and confidence of the users as well as the businesses [6]. In this regard, even multinational companies are struggling to handle data collected related to digital sales; part of digital exploitation is that any document is readily available over the internet and some software is automatically downloaded even without the consent of the user which results in information stealth. In the B2B sector, there is a desire for a secure connection, secure transfer of data, and establishment of a secure digital platform while the distinction between the technical and economic platform operators is a must who play intermediary roles [7]. Industrial consortia and cooperatives are examples of such platforms which form the core of smooth operations of the interfaces and IT infrastructure between two businesses. These platforms collate all the information in a virtual database where responsibility is taken for invoicing, pricing, shipping, and contract negotiation[10]. If these platforms are fair and act as gatekeepers, then digital sovereignty can be guaranteed but in case these platforms and operators steal information, there should be allocation of a separate digital platform for each business.

There are various degrees of digital sovereignty which can be low, medium, or high for companies. When the data can be deleted or altered by the company, then there is no dependency on other companies or national digital platforms provided, and thus high digital sovereignty is maintained (Bendig et al, 2020)[10]. In B2B sales, when the online platform can be operated without any approval of distribution and federation agencies, then digital sovereignty is ensured and vice versa. The interfaces must be freely available with open-source reference implementation and if the source code of the software can be altered independently then there will be high digital sovereignty [8]. If all the technical and hardware components can be provided in the EU with complete technical control by businesses then B2B sales will incur more digital sovereignty; moreover, the B2B sales can increase if businesses have skills to access and evaluate existing players.

There are several advantages of implementing digital sovereignty in B2B sales including consumer confidence, loyalty, goodwill, and brand equity as consumer confidence is raised and he feels confident in making purchases from such retailers. The company has the potential to increase its revenues and profits after having control over data [9]. The challenges of implementing digital sovereignty include huge costs on a national level as the EU and governments, in general, will incur huge capital costs to inculcate digital sovereignty. There should be the removal of barriers in creating own data platforms for companies.

Prospects

There is a need for improvement and government actions to support digital sovereignty. Infrastructure must be built up to support the companies who wish to have separate digital platforms for their businesses. To incorporate digital sovereignty, there should be given access to remote data to every business and the availability of the services should only be made through eID and governments must make sure that the owner of data can set level of requirements with no authentication strings and internal mechanisms [10]. The security features and platforms should be adequately and equally available to everyone so that B2B sales can be conducted and even the software for users or clients must be provided which they can install in tablets, laptops, and PCs. It should be made possible that the data and documents are encrypted and cache of active elements must be done after a certification process in the user environment [11]. Any operation that needs server-side processing must be made unavailable by businesses so that the rights of B2B clients are protected. In the B2B sector, there is a strong need for the establishment of integration modules, data-sharing platforms, and IoT platforms that collect big data in the factory for manufacturing companies with each company using suitable software applications.

Conclusion

The digital platforms have helped businesses in targeting new markets and consumer segments with the ability to increase potential revenue. However, digital sovereignty involves the protection and control of data so that companies can manage and use data on their own with no fear of data exploitation. The hackers and cybercrimes nowadays have made the online environment worse by invading the privacy of consumers; as a solution, the EU is planning to invest in technology-based programs which give credence to the sovereignty of the masses. In the B2B environment, there are platforms available that can control and manage information along with negotiation of prices for products and services but these platforms must be

secure. The B2B sales can increase if companies have their interfaces and databases so that the clients feel secure resulting in enhanced financial performance. For the future, there is a need for B2B platforms to use their independent data-sharing interfaces, AI, and the Internet of Things so that transparency can increase.

Notes

[1] **Harris Interactive Survey.** *« Big Data », qu'en pensent les Français ? – Enquête*. 2016, <https://harris-interactive.fr/opinion_polls/big-data-quen-pensent-les-francais/> (9 August 2021).

[2] **Pohle,** K. *Digital sovereignty*. // www.kas.de. 2020, <https://www.kas.de/en/single-title/-/content/digital-sovereignty> (9 August 2021).

[3] **Madiega,** T. *Digital sovereignty for Europe*. // EPRS Ideas Paper. 2020, <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf> (9 August 2021).

[4] **McKinsey Report.** *The B2B digital inflection point: How sales have changed during COVID-19*. 2020, <https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/the-b2b-digital-inflection-point-how-sales-have-changed-during-covid-19> (9 August 2021).

[5] **Davie,** C., **Stephenson,** T. **and De Uster**, M.V**.** Three trends in business-to-business sales. *McKinsey Quarterly*, 2010, *19*(1), pp.1-4.

[6] **Bria,** F. Public policies for digital sovereignty. Platform Cooperativism Consortium conference, 2015, New York.

[7] **Montaigne Institute.** *Digital Compass: Europe's Digital Sovereignty?*. 2020, <https://www.institutmontaigne.org/en/digital-compass-europes-digital-sovereignty> (9 August 2021).

[8] **Hobbs,** C. Europe's digital sovereignty: From rule maker to Superpower in the age of US-China Rivalry. // Ecfr.EU. 2020, <https://ecfr.eu/wp-content/uploads/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf> (9 August 2021).

[9] **Dellinger,** A. *Personal Data Of 533 Million Facebook Users Leaks Online*. // Forbes. 2021, <https://www.forbes.com/sites/ajdellinger/2021/04/03/personal-date-of-533-million-facebook-users-leaks-online/?sh=42bb332d717c> (9 August 2021).

[10] **Bendig,** T., **Biener,** R., **Dapp,** E., **Ehmann,** T. **and Ganten,** V. *Digital sovereignty in the context of platform-based ecosystems: The Digital Sovereignty Focus Group of the Innovative Digitisation of the Economy Platform for the 2019 Digital Summit*. // Federal Ministry for Economic Affairs. 2020, <https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/digital-sovereignty-in-the-context-of-platform-based-ecosystems.pdf?__blob=publicationFile&v=7> (9 August 2021).

References

1. **Floridi,** L. The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33(3), 2020, pp.369-378.

2. **Ilves,** L. and **Osula,** A. The Technological Sovereignty Dilemma – and How New Technology Can Offer a Way Out, *European Cybersecurity Journal*. 6 (1), 2020, pp. 24-35.

3. **Halpin,** H. Digital Sovereignty. *Multitudes*, 35 (4), 2008, pp.201-213.
4. **Lambach,** D. The Territorialization of Cyberspace. *International Studies Review*, 22(3), 2019, pp. 482-506
5. **Burri,** M. The Regulation of Data Flows through Trade Agreements. *Georgetown Journal of International Law*, 48(1), 2017, pp. 408–448.
6. **Mollers,** N. Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State. *Science, Technology, & Human Values*, 46(1), 2020, pp. 112–138
7. **Cavelty,** M. D., **Egloff,** F. J. The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony's International Review,* 15(1), 2019, pp. 37–57.
8. **Mueller,** M. Against Sovereignty in Cyberspace. *International Studies Review*, 22(4), 2020m pp. 779–801.
9. **Pasquale,** F. Two narratives of platform capitalism. *Yale Law & Policy Review*, 35(1), 2016, pp. 309–321.
10. **Posch,** R. Digital sovereignty and IT security for a prosperous society. In *Informatics in the Future*, 2017, pp. 77-86. Springer, Cham.
11. **Werthner,** H. and **van Harmelen,** F. *Informatics in the Future: Proceedings of the 11th European Computer Science Summit (ECSS 2015), Vienna, October 2015* (p. 109) 2017, Springer

About the author

Mostapha Bouyrakhen received his first Diploma in 2004 from the University of Applied Sciences Frankfurt am Main in Computer Science and Engineering and gained his first international Sales experience in the UK for more than one year and continued with a Master of Business and Engineering (MBE) degree at Steinbeis University Berlin. He has 14 years of experience in International B2B Sales and advanced knowledge in general and sales management combined with intercultural competences.

To contact the author: m_bouyrakhen@yahoo.de