Three Acts

Prepared by Hosuk Lee-Makiyama, Director of ECIPE assisted by Claudia Lozano.

Originally published by the Wilson Center [link]. ZPP thanks Dr Dan Hamilton and the Wilson Center, Washington D.C. for the kind permission to reprint the article

We would like to express our gratitude to Mr Hosuk Makiyama, director of European Centre for International Political Economy (ECIPE) for opportunity to share the reprint of the article and his guidance.

At the end of 2020, the European Commission had tabled no less than three new acts with the goal of regulating its digital markets. With a stated objective to create a safer digital space where fundamental rights of all users of digital services are sufficiently protected, the Single Market changes its mode of market governance from addressing market failures ex-post (as they happen) that are tailored to create the same outcome.

The three acts – Digital Governance Act, Digital Services Act and Digital Markets Act – builds on the political successes of the General Data Protection Regulation (GDPR) and the political capital it has unleashed to act against digital-native players. But they depart from the philosophy of GDPR, a horizontal regulation that applies to all societal processes involving personal information, whether they occur online or offline – or by public, private or commercial actors. Instead, the three digital acts are detailed product or activity-specific regulations that only apply to some digital market actors.

Under such circumstances, suspicions of digital protectionism are never far away. The preambles and justifications contain language or references to "level playing field", or the objective to encourage innovation, growth, and competitiveness. The EU Member States, or even the Commissioners themselves, are divided on the merits of the three acts: After all, addressing alleged markets failures via detailed regulations erode the European Commission's exclusive powers on antitrust investigations. The legislative process is expected to take several years, consuming resources and political bandwidth from other legislative work. There are also legitimate concerns about being mired down in trade disputes.

This note illustrates the key features of the three acts. In addition, the EU is still in the midst of an overhaul of the e-Privacy Regulation that protects personal data in electronic communication; a regulation on artificial intelligence is due in April 2020; while the plans for a digital levy (a de facto union-wide corporate income tax that is specific to online services) is essentially the rescinded Digital Services Tax (DST) in a new form.

Digital Governance Act (DGA)

The stated objective of the DGA is to improve data sharing conditions in the internal market, promote confidence in data sharing while ensuring compliance with data protection laws and breaches of confidentiality. DGA is effectively an appendix to the GDPR, and its subsidiary standing is even explained in its provisions.

It lays a new foundation of the data governance model across three pillars of its application:

- Protected data held by public bodies, i.e. regulating a specific type of data
- Data sharing businesses (including European Data Spaces or personal data-sharing intermediaries), i.e. regulating a specific type of activity
- Data altruism (e.g. use of data for non-commercial or altruistic reasons), regulating a specific purpose.

Although the initial proposals contained provisions that force localisation of data within Europe, such provisions have been dropped before the publication of the legal drafts. Nonetheless, the provisions will be subject to intense discussions internally. The majority of the concerns are raised on the second pillar of the Act on "data-sharing". This elusive definition is largely understood to mean "data trusts" and other future data intermediation activities (i.e. not today's online platforms). By and large, it is understood to mean any activity that overlaps in scope with Gaia-X (the Franco-German data trust and PPI partnership).

Data-sharing services may not provide any other services than data-sharing, and any other service must be put into a different legal entity. Moreover, the DGA includes a notification procedure and monitoring of compliance by the appropriate authorities of each Member State.

Therefore, the requirement is a de facto licensing requirement for data-sharing activities. Although the notification is largely pro forma, non-compliance could also lead to cessation of that service. For altruistic purposes, the registration requirement is voluntary.

More broadly, the DGA regulates "sharing" as an activity rather than on the basis of a data object (e.g. personal information). Therefore, there will be situations where the DGA could conflate GDPR with non-personal data. DGA already restricts sharing of non-personal data that must not be shared from an EU country to a third country without an imposition of 'adequate safeguards' aiming at ensuring the protection of fundamental rights or interests of data holders. Similarly, public data may only be transferred to third countries with adequate IPR protection.

As DGA does not offer any new incremental protection of data beyond GDPR or intellectual property rights, the actual value for citizens or rightsholders will be disputed. Moreover, DGA does not contain provisions defining territorial scope. Non-EU services must appoint a legal representative within the Single Market.

Finally, European public data may not be subject to exclusive arrangements that can be anti-competitive, which will be positive for fostering big data applications building on public data. However, the DGA also provides a legal basis for the Member States to impose further obligations for re-use of any protected data (held by public bodies) on the grounds of commercial and statistical confidentiality, privacy or IPRs.

Digital Services Act (DSA)

The DSA aims at framing a single set of new rules applicable across the EU. It "updates" the E-Commerce Directive from 2000 that regulates the liability of intermediaries for illegal content. It applies in addition to the E-Commerce Directive and the P2B Regulation of 2019, and the DSA will also be applied through national implementations.

The DSA applies to online intermediary services, including internet access providers and entities offering network infrastructure, hosting services and online platforms that connect sellers and consumers such as online marketplaces, collaborative economic platforms and social media platforms.

Rules and obligations differ based on the company's size and are proportionate to their ability and size while ensuring they remain accountable. Among the new requirements found in the DSA, all services must abide by transparency reporting and fundamental rights obligations. They are also required to cooperate with national authorities when necessary. Like the DGA, the DSA

also involves the establishment of points of contact and the requirement to designate a local legal representative for non-EU entities.

Very large online platforms, with more than 45 million monthly users in the EU, must follow additional requirements (contained in its own section of the Act), including the provision of systemic risks (e.g. illegal content, privacy violations) and address them with effective content moderation mechanisms. They must also maintain a public repository with detailed information of online advertisements, designate a compliance officer and, upon request from the competent authorities, provide data necessary to monitor compliance with the DSA. These requirements also impose high fines (up to 6% of its total turnover in the preceding financial year, where it finds that the platform has intentionally or negligently violated them).

Any legislation concerning content or service provision liability requires clarification on the definition of illegal content. Some parties also argue that there ought to be differentiation in approaches to illegal content online and content moderation disputes.

Digital Markets Act (DMA)

DMA is arguably the most controversial of the three acts. Drafters of the Act state their intention to address "digital market imbalances that arise from gatekeeper platforms" through harmonised rules, prohibition of discriminatory practices by gatekeeper platforms and provides enforcement mechanisms based on market investigations.

The DMA will apply to online platforms, including social networking services, operating systems and online intermediation services, while offline intermediaries (multi-brand retailers, convenience stores, brokerages) are exempt. By and large, gatekeepers may not treat their own products more favourably in the ranking than similar services or products offered by third parties. Also, gatekeepers may not prevent consumers from linking up to businesses outside their platforms and prevent users from uninstalling any apps.

Further criteria set out by the European Commission defines a "core platform services provider" when a gatekeeper meet the following criteria:

- Significant impact on the internal market and present in at least three EU Member States. Annual turnover in EU/EEA exceeding EUR 6.5 million.
- Strong intermediary positions, i.e. more than 45 million monthly active users and more than 10,000 yearly active business users in the EU;
- Stable and durable market position, i.e. businesses that follow the previous criteria for the last three financial years minimum.

Specific obligations for very large online platforms include stricter transparency and reporting obligations. Consequently, an online platform that holds a small corner of several Member States will be subject to new regulatory action, whereas a major player that only operates in a Member State is exempt. A perverse consequence of these criteria is how an online platform may be penalised for utilising the Single Market and the internal market of services while national market dominance is rewarded. Also, illegal content and products will merely be pushed to small digital service providers.

Other criticism includes concern over the DMA seeking to disrupt the core services of so-called digital 'gatekeepers' by restructuring their relationship with business users and imposing new terms and obligations with both far-reaching structural and behavioural remedies (including divestiture) in addition to fines up to 10% of the company's total worldwide annual turnover or periodic penalty payments up to 5% of average daily turnover.