THOUGHT LEADERSHIP

TECHNOLOGY, MEDIA & ENTERTAINMENT

DATA ANALYTICS & PROFILING– WHAT SHOULD THE LAW DEMAND?

PART II

Jackson, Etti & Edu

Technology, Media & Entertainment

Part Two

Outline

- **What is the Position of the GDPR on Data Analytics and Profiling?**
- **What is the Position of the NDPR? Is Data Analytics and Data Subject Profiling Allowed?**
- **Emerging Technologies & Tools**
- **Should There be New Compliance Requirements? What Should the Law Demand?**

The first part of this article discussed the concept of personal data and the nitty-gritty of data analytics and data profiling, both from an industry and legal perspective. This present part explored the current legal framework, its impacts, and the way forward for regulations on Data Analytics (DA) and Data Profiling (DP).

You can read the first part of this article here

What are Data Analytics and Data Profiling?

The General Data Protection Regulation (GDPR) prohibits solely automated decision-making – including profiling [1] - which has legal or similar effects on the data subject. [2] Article 22(1) of the GDPR specifies the exceptions to the restriction, namely:

1. necessary for entering, or performance of, a contract between the data subject and a data controller;
2. authorised by the law; or
3. where the data subject gives express consent [3]

-The question is what type of profiling or decisions have legal or similarly significant effects?

Decisions have legal effects when they can affect the legal rights or benefits of the data subject. For example, a decision to provide accessibility to a government-insurance scheme. Decisions with similarly significant decisions are not close-ended, and they may affect the data subject's reputation, recruitment opportunities, health, financial status (e.g., loan application, credit scores), and (predictions on) choices/behaviour.

[1] Art. 4 (4), GDPR defines "profiling" as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."
[2] Art. 22(1) and Recitals 15, 63, 68, 71, GDPR
[3] Art. 22(2), GDPR

As mentioned earlier, the effects of wrong or discriminatory solely automated decision that has legal or similarly significant effects on the data subjects can be severe, especially when children are involved. As such, data protection regulators in Europe have been forced to crack down on companies for data breaches. While no company has been directly cited for breaching Article 22(1) of the GDPR, the citation and fine imposed by the German authorities on H&M is a bit similar to the subject matter in focus.

H&M had asked employees who went on vacation or sick leave to attend an interview on resumption to work. This process allowed H&M senior managers to gain access to private information about their staff. The personal information was then used to develop profiles on the employees and subsequently used to evaluate their performance and make decisions about the employees.

The Data Protection Authority of Hamburg cited H&M for breaching the GDPR's principle on data minimisation and for making employment decisions based on the personal information collected from the concerned staff members without their consent. The authorities imposed a fine upwards of €35m and this is the second-highest fine by a national authority in Europe.[4]

-What are the best practices for controllers to demonstrate compliance with the GDPR requirements for solely automated decision-making including profiling and with legal or similarly significant effects?

---

[4] Tessian, "18 Biggest GDPR Fines of 2020 and 2021 (So Far)" accessed via https://www.tessian.com/blog/biggest-gdpr-fines-2020/ on 19th June 2021.

a. Where consent is used as the lawful basis, the following checks can be put in place to demonstrate compliance, in addition to the conditions underlisted under paragraph (b) below.[5]
    i. Require explicit consent from the data subject
    ii. Record the subject's consent
    iii. Inform and provide features for the subject to withdraw consent
    iv. For children, there must be parental consent[6]
b. Under any of the exceptions to the restriction on solely automated decision-making with significant effects, the following conditions can be fulfilled to demonstrate compliance:
    i. Inform in plain and simple language what and how the data collected will be processed for DP and how it can have a significant effect on the subject
    ii. Inform the subject of the right to object to the processing or the outcome
    iii. Halt processing and inform the data subject of the discontinuance within a month from the date the processing was discontinued
    iv. Provide the subject with the mechanism to object to the processing or challenge the outcome and request human intervention
    v. Provide the subject with a report on data being processed upon request or within a reasonable period
    vi. Name the organisation and third-party controllers/processors that will have access to the data[7]
    vii. Employ appropriate mathematical or statistical procedures for the profiling
    viii. Implement technical and organisational measures appropriate to ensure minimised risk of errors and inaccuracies i.e., conduct a Data Protection Impact Assessment (DPIA) before processing data in such a manner
    ix. Put necessary security in place to prevent discriminatory effects on natural persons or unfair decisions[8]

Although there are three categories of exceptions (already discussed above), there is a consensus among data protection regulators and experts that properly obtained consent remains the best lawful basis for processing data in any way.

What is the Position of the NDPR? Is Data Analytics and Data Subject Profiling Allowed?

The Nigeria Data Protection Regulation (NDPR)[1] recognises automated processing of data (DA) and automated decision-making that includes the profiling of data subjects (DP).[2] Unfortunately, the NDPR does not define "(solely) automated decision-making" or "legal effects" or "similarly significant effects".[9]

---

[5] Art 22(4), GDPR
[6] Information Commissioner's Office, "Consent" accessed via https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ on 20th June 2021
[7] Ibid.
[8] Art. 71, GDPR
[9] The NDPR was released by the National Information Technology Development Agency in January 2019 to address the privacy concerns and rights of citizens

Unlike the GDPR, Article 5.3.1 (f) of the NDPRIF states that the data subject's consent as the only lawful basis for solely automated decision-making with a legal or similarly significant effect on the subject.[10] Article 5.3.2 of the NDPRIF further specifies that explicit consent [11] is required in the processing of sensitive personal data.[12] There are also guidelines to be followed by controllers and the rights of data subjects in the circumstance.

-NDPR Guidelines to be Followed by Controllers and Administrators Involved in Data Profiling

The NDPR and its Implementation Framework (NDPRIF)[13] provide the following guidelines to safeguard the rights of data subjects where data processing is done by an automated means and results in an outcome that have legal or similarly significant effects on the subject.

a. Data subjects must be informed transparently on the use of automated decision-making that includes profiling and the significance and possible consequences of such processing [14]
b. Data subjects have the right to request, receive or transmit personal data under this category (Data Portability) [15]
c. The right to object to such processing [16] or challenge the accuracy of the personal data [17]
d. Controllers must communicate in clear terms the procedure for subjects to exercise their rights to object or challenge the processing or outcome respectively [18]
e. Controllers and Administrators may be required to carry out a DPIA before conducting a solely automated decision-making process with legal or similarly significant effect [19]
f. Controllers and Administrators required to file the annual audit report to NITDA must also include the existence of solely automated decision-making processing, including profiling, the significance and the possible consequences of such processing on the subject [20]

It is important to note that controllers and administrators must observe other duties imposed by the NDPR and the NDPRIF e.g., publication of a privacy policy, data minimisation, cross-border transfer of personal data.

---

[10] Lawful bases for data collection and processing under the NDPR include:
[11] Art. 5.4, NDPRIF defines explicit consent as a clear, documentable consent e.g., ticking of boxes, a sign-up, request by email, etc.
[12] Reg 1.3(xxv), NDPR defines "Sensitive Personal Data" as "data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information"
[13] NITDA released the NDPRIF in July 2020 as a follow up to the NDPR and serve as a blueprint to compliance with the principal regulation.
[14] Reg 3.1(7)(l), NDPR
[15] Reg 3.1(14), NDPR
[16] Reg 3.1(11)(d), NDPR
[17] Reg 3.1(11)(a), NDPR
[18] Reg 2.8, NDPR; Art. 3.2(xvii), NDPRIF
[19] Art. 4.2(b), NDPRIF
[20] Art. 6.6.1(l), NDPRIF

Criminal sanctions for non-compliance include (in addition to any other criminal liability):

1. a fine of 2% of the Annual Gross Revenue of the preceding year or payment of the sum of 10 million Naira, whichever is greater in the case of a Data Controller dealing with more than 10,000 subjects
2. a fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of 10 million Naira, whichever is greater in the case of a Data Controller dealing with less than 10,000 subjects[21]

Emerging Technologies & Tools

The emergence of innovative technologies in Data Analytics and Data Profiling promises a robust potential for market growth and revenue for companies willing to go the extra mile to analyse higher volumes of data at higher speed, resulting in what is known as Big Data Analytics. These disruptive technologies are further powered by already existing technological inventions such as ML, analytic and decision-making algorithms, IoT, AI, etc.

Major beneficiaries of DA and DP technologies are fintech, health, Big Tech companies (especially social media companies), fast-food franchises, and real estate companies.

A scenario is that by simply surfing the internet for a bag to buy with the use of an internet-enabled mobile device, an individual A can leave several digital footprints (e.g., keywords, cookies, order history, spending patterns) that can be picked up by IoT (e.g., cookies) and analysed by ML or AI tools of a social media company such as Facebook or Instagram or the search algorithms of Google or Yahoo search engines. This is not the end. This data can be collated, analysed and transmitted to third-party sellers to create targeted advertisements for A.

[21] Reg 2.10, NDPR

On a larger scale, higher traffic or volume of data from different individuals in the same location of A within the same age group can be collated and analysed to predict their income range. With the acquisition of this information, a Fintech company can carefully determine the type of service offerings to offer this class of people and target ads at them and subsequently automatically include or exclude them from some categories of e-loan applications or insurance scheme offerings.

However, problems may begin to arise in this smooth process if:

- the middleman DA company or the third-party seller or the fintech company becomes overdriven by profits and pays no attention to the privacy of subjects
- the data collated is inaccurate
- the decision-making algorithm or analytic tool is based on the wrong logic for such decisions or is susceptible to external breaches (hacks)
- data subjects are being discriminated against and unfair decisions are made without recourse from the subjects

Should There be New Compliance Requirements? What Should the Law Demand?

Again, it is important to emphasise that regulators must not take an adversarial or aggressive stance against disruptive technologies that support Data Profiling. The aim should be to build trust in the processes developed by organisations through guidelines for best practices and enforcing the law on erring companies.

To achieve this, the following recommendations are made to ensure DA and DP processes in companies are healthier in Nigeria as well as the data protection framework:

1. introduce the right of subjects to challenge outcomes of solely automated decision-making processes and request human intervention into the provisions of the NDPR
2. mandate controllers to embed control measures in their processes and tools to verify the accuracy and quality of data inputs when conducting Big Data Analytics
3. mandate human intervention for all automated decision-making processing in health diagnosis and treatments
4. increase the penalties for breach of the specific provisions on automated decision-making processes

---

Ibid

Elizabeth D., "Big data, artificial intelligence, machine learning and data protection" Information Commissioner (2017) accessed via https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf in 19th June 2021.

Other non-legislative steps the regulators may take, include:

i. engaging all the stakeholders to know the pros and cons of new policies to foster the development of this industry and how to address the negatives of an unregulated industry
ii. sensitisation of the public on their rights to data privacy and the mechanisms in place to file complaints against erring companies

It is hoped that not only the regulators but organisations that fall into the scope of the NDPR pay more attention to the quality of data inputs and also take the rights of data subjects more seriously.

Author

Olusegun Oyesanya
Associate
e: segun.oyesanya@jee.africa

Key Contacts

For more information, kindly reach the key contacts below:

Ngozi Aderibigbe
Partner & Sector Head, Technology, Media & Entertainment
e: ngozi.aderibigbe@jee.africa

Yeye Nwidaa
Sector Co-Head, Technology, Media & Entertainment
e: yeye.nwidaa@jee.africa

Contributors:

Tobi Opawoye
Joy Azumara
Collins Mbakwe
Seun Fadairo
Onyedikachi Okocha

Jackson, Etti & Edu

RCO Court 3-5, Sinari Daranijo Street, t: +234 (1) 4626841/3, +234 (1) 2806989 f: +234 (1) 2716889
Victoria Island, Lagos, Nigeria. e: jee@jee.africa www.jee.africa