LawDigits
Education | Research | Innovation

THE DATA SUBJECT'S RIGHT TO BE FORGOTTEN

Practical Course for Data Privacy Professionals

Created By: Oladipupo Ige admin@thelawdigits.com

General Learning Objectives

By the end of this course, participants will understand the legal foundations of the Right to Be Forgotten and the lawful grounds upon which personal data may be erased. They will be able to assess real-world erasure requests, recognise key limitations and exceptions, and evaluate organisational compliance obligations.

Participants will also gain practical insight into drafting and assessing internal erasure policies, equipping them to confidently balance privacy rights with competing legal and public interest considerations in today's digital landscape.

Want to know more about LawDigits?

Follow us on our social media pages.

COURSE OUTLINE

The Right to be Erased

Module 1: INTRODUCTION TO CONCEPT

Module 2: THE RTBF AND CBDT

Module 3: RTBF AND THE ORDEAL OF THE REHABILITATED CRIMINALS

Module 4: RTBF UNDER THE NIGERIAN LAW

Module 5: RTBF IN PRACTICE, OPERATIONAL CHALLENGES & RECOMMENDATIONS

What is the Right to be Forgotten?

Simply put, the right to be forgotten is a **right of a data subject to have private or personal data removed from any directory, both physical or online.** This directory includes search engines, websites, advertisement columns, email leads for companies, employee payment list, subscription lists etc.

It is the right to have your personal data removed and excluded from further processing.

This can occur when a person requests for his/her data to be deleted so it can no longer be discovered by third-parties or by search engines.

It is the revocation of the access to specific information that was publicly available or that was being used for processing by a data controller. The right to be forgotten is not merely a data protection issue, it is a major privacy concept that has been debated over the years.

Should people be allowed to control which data related to them are published and how long this published data can STAY PUBLISHED?

Reasons why a Data Subject might want to be Forgotten

- Potential/Current Harm to Reputation i.e., political views, court cases, affiliations, affairs, employment, marital etc.
- Running from the Past i.e., criminal activity, previous comments, unscrupulous activities.
- Social Media Pressure i.e., Break from social media activities or spotlights, Information leak. Artificial Intelligence.
- To halt simple data processing for legitimate, consensual or contractual purposes.
- Inaccurate or incorrect data.

Adunni Ade I Wolfgang Werlé I Costeja I Biancardi

HushPuppi I Ed Gein I Sexual Offenders I Axel Springer

Very Dark Man Location Leak I Simi & Ezra I SoraAI

MTN I E-Cart I Google I Advertisement I Seedance

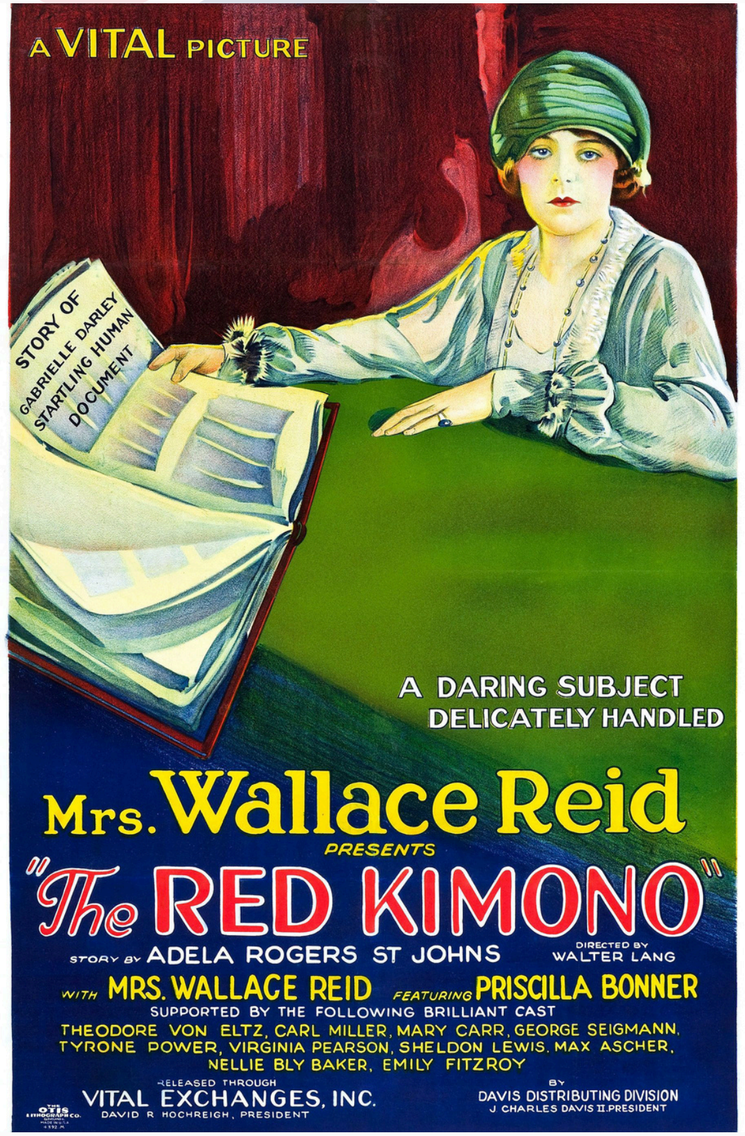
Public Records I Certificates I BVN I NIN

History of the Concept

The issue of the RED KIMONO

The RTBF can be traced to the case of **Melvin v. Reid (1931)** where an ex-prostitute that was involved in a murder case wanted to live a quiet life after all the life of hustle. A movie producer then made a movie with her story and she sued that the movie was a violation of her right to privacy. The court ruled that she had a right to be away from public. In the Judge's words, **"any person living a life of rectitude has that right to happiness which includes a freedom from unnecessary attacks on his character, social standing or reputation"**

Fast forward to the modern age. The first time I heard the concept of RTBF was in the book "Surveillance Capitalism" by Shoshana Zuboff. In the book, she mentioned a case in 2014 againt Google that occurred in Spain. Many people do attribute this case to the beginning of RTBF as an established concept in the behavioural surplus market. I beg to differ. There was a case in Argentina that first sparked the plug and laid a foundation for the EU case known today as the **COSTEJA case**. To properly appreciate the topic. It is necessary to discuss these cases and how they affect the concept of the right to be forgotten. The aim is to give a robust overview of the concept.



RTBF and its Historical Cases

Virginia De Cunha

Virginia De Cunha 2009 Case – Argentina

The lady was an actress and a musician. She had consented that some pictures of her be posted on the internet. However, these pictures were posted by pornography websites and the links appeared as search results on the platform of Google and other search engines. She sued that Google damaged her reputation and requested that such searches and the links be filtered out from obtainable search results. The Supreme Court asked;

HOW CAN YOU GUARANTEE THE FREE CIRCULATION OF INFORMATION AND IDEAS ON THE INTERNET IF YOU BLOCK SUCH SEARCHES?

The Supreme Court ruled that **a search engine does not have any liability for the results the search engine produces** and that the use of a filter to block results would amount to **CENSORSHIP**. The court stated that the **third party websites that own that content** should be solely liable. **This ruling meant that search engines are allowed to produce any result on the internet regardeless of the harm it poses to reputation or privacy without liability.** This created the argument of intermediary liability for natural search results.

Reflections

1. What about instances of advertisement?
2. What if the search engine company got paid to push and advertise the content?

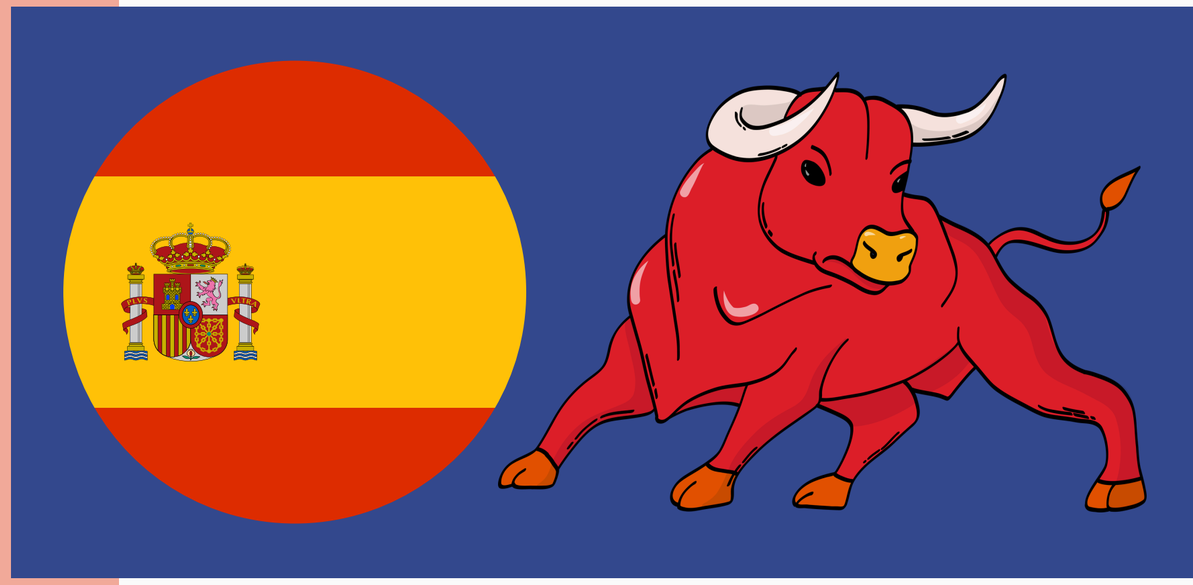
LawDigits
Education | Research | Innovation

LawDigits is a data privacy hub for educational materials, data protection training and consultation. To know more about us, kindly follow us on LinkedIn YouTube

The decision was refined in the **Baidu** case in China. The search engine associated the man with his former employer. This was in 2016. The court held that search results are **“neutral findings based on algorithm and stated that retaining such information was necessary for the public”**. Years after the case, China passed the National Standard of the People’s Republic of China on Personal Information Security Specification and included a right to be forgotten.

However, the **COSTEJA** case in Spain presents another perspective on the possibility of the right to be forgotten online. In that case, a lawyer listed some properties online for sale. Years after the sale had been concluded, whenever the lawyer was googled, the listing link presents itself. The man then sued. The CJEU in deciding the case stated that **“internet search engines must consider requests from individuals to remove links to freely accessible web pages regarding name searches”.** The grounds for removal of the search result includes; when it is **inaccurate**, **inadequate**, **irrelevant** or **excessive.**

Google Spain v. Gonzalez



This led to the creation of the **removal request form** on google. The Applicant will fill a webform and request for deletion. It is then subject to review by algorithm and also human assistance. The request can either be approved or refused,in which case, the content stays online. There is a google appointed advisory council for the oversight function of this content removal scheme.

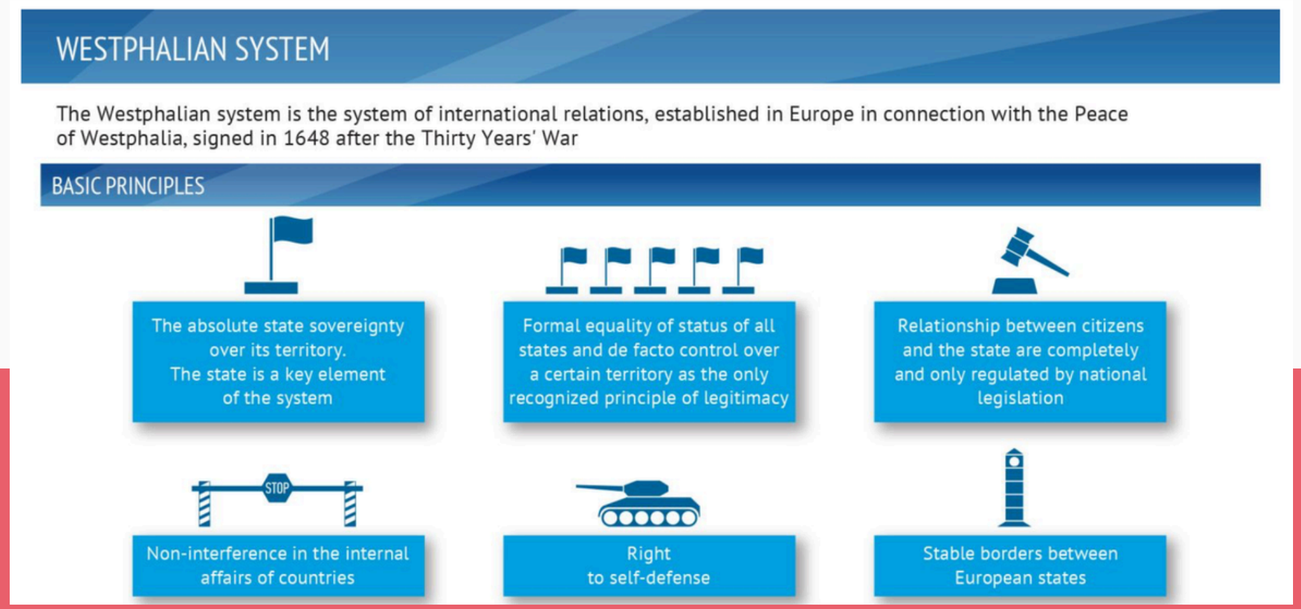
CHECK TEMPLATE

Reflections

1. Isn't this self-regulation/governance by data controllers?
2. What is hope of the common man?
3. How does this impact freedom of expression and the press? Are internet information accurate if some are filtered? Won't people try to take advantage of this law to remove content they find distressing about them online? What about AI?
4. Is the company obligated to delete content in other countries?

THE RTBF AND CBDT

Well, to begin, we need to understand the concept of territory under international law. Simply put, the reach of a country's jurisdiction is limited to its geographic territory. This is known as the **WESTPHALIAN SYSTEM** under international law. It's a system designed in **1648**.



In modern day, the internet does not respect this Westphalian rule made 378 years ago. Online interactions are independent of geographic location.

Therefore, if a data subject obtains judgement for content removal in a country, does that mean people in another country would also not have access to the removed content?

What if it is information that is relevant in another jurisdiction? Basically, does this law have extra-territorial effects if the fellow is not in an EU country?

Professor. Victor Schonberger

Some scholars like Professor Schonberger has stated that the law, particularly, in **France** must also apply to other jurisdictions. To address this issue, the EU and USA signed a data transfer agreement. They used to call it the **SAFE HARBOUR PRINCIPLE** or Rule. This was around 2000s. In 2015, the Schrems case threw the principle out of existence and termed it inadequate.

The safe harbour principle was a self-declaration by American firms that they will protect personal data in their custody and basically a form of adequacy notice between EU and USA. CBDT can only take place if the company complies with these rules. However, in 2015, a lawyer sued that this method was inadequate citing the **Edward Snowden** whistleblowing on American surveillance around that period. **The CJEU held that the safe harbour principles were insufficient to address data protection concerns.**

Currently, a form of adequacy notice is still used.. It is now called the **PRIVACY SHIELD PRINCIPLES**. The principle specifically provides for the option for the data subject to **"opt out"**. This means that such data related judgements are applicable in both jurisdictions. This in effect would mean that any country that has adequacy notices or some form of BCR or SCCs with the data controller company or the company's country will also be subject to the decision regarding the right to be forgotten.

This invariably connotes that the content is removed and data processing ceases across board. This is extended to all third parties or data processors thus resolving the issue of cross-border application of RTBF.

Now, they use the **EU-US Data Privacy Framework (DPF)**.

In 2025, the **right to be forgotten (RTBF)** is under heightened scrutiny, with the European Data Protection Board (EDPB) conducting a major, coordinated enforcement initiative across the EU/EEA, examining how 40+ organizations handle erasure requests.

This initiative focuses on the practical application of GDPR Article 17, as it is a frequent source of complaints.

Areas of interest include online data of Children, Access to Financial Services, Health status, etc

RTBF AND THE STREISAND EFFECT

Another concept in the right to be forgotten is the **Streisand Effect**. It is a situation where you are trying to avoid a breach of your privacy and due to your actions to prevent, you proliferate the event, narrative or content. This came about as a result of the 2003 case of Barbra Streisand. She sued to remove the picture of her house from a malibu photoalbum. Due to the case and her status, the photo of the house ended up in numerous media spaces that it was practically impossible to remove them all.

So the question is, in such instances, doesn't the right to be forgotten further exposes the privacy of the person attempting to prevent a publication or content from affecting reputation, causing harm or preventing surveillance by directing attention to the privacy matter?

Reflections

1. Are there ways to address this?
2. Can court judgements or data in possession of the court be subject to the right to be forgotten?
3. How does this work in AI?

LawDigits
Education | Research | Innovation

Want to know more about data subject rights?

We offer courses and interactive online classes for data privacy professionals.

Learn history of laws, current trends and practical methods of implementation available in the data protection field.

LEARN MORE **FOLLOW US**

RTBF AND THE ORDEAL OF THE REHABILITATED CRIMINALS

Can the right be forgotten be exercised by persons convicted of crimes such as sexual offences, theft, murder etc.? Instances where this might be necessary are those that involved employment, access to social amenities and other benefits.

How does this affect freedom of expression, media and journalism?

In 2009, the German courts were saddled with the **Wolfgang Werle case**. Two brothers were involved in the murder of an actor – Sedlmayr in 1990. The actor was tied up, stabbed in the stomach and his head was battered in with an hammer. The case of the **Berliner Morgenpost**.

The brothers were sentenced to life imprisonment. When they were eventually released in 2009, Wolfgang sued Wikipedia and requested that his name should be suppresed from publications. They also sued some German websites.

In determination of the matter in 2018, the European Court of Human Rights ruled that the lower court was right to reject the request to ban publications of the killer's names and stated that; **"The approach to covering a given subject was a matter of journalistic freedom, and reporting individualised information was an important aspect of the press's work".**

A notable decision is the **LUXEMBORG CASE** that involved the President of the Trade Union that was convicted of bribery and corruption. After 20 years of the issue, some journalists raised the issue and named the ex-convict in their piece and even in a TV interview. The man sought to be forgotten and took the matter to court. The district courts held that they needed to balance two rights.

The right to privacy and freedom of expression depending on the interest at stake, and to prioritize the solution that most protects the most legitimate interest. The district court ruled that he should be forgotten.

The matter was appealed and the Court of Appeal upheld the decision.

The court explained that consideration had to be given to the contribution of the publication to a debate of **general interest**, **the notoreity of the person concerned**, **their previous behaviour**, **the content**, **the form** and **the impact of the publication** to assess whether a restriction of press freedom was justified because it pursued a legitimate goal that was proportionate.

The court said the matter related to judicial history so it's a debate of general interest but held that the publication of his image or name were not necessary to achieve the legitimate goal of informing the public.

The man had served his sentence, has retired from public office and had no particular public relevance therefore there was no need to publish his image or his name to tell the story. So it became a matter of proportionality and the type of crime committed. This is a much better decision than the Wolfgang case.

To know more, read the Axel Springer v. Germany or Biancardi v. Italy cases

For criminals in the UK, details of criminal convictions are not considered when obtaining insurance or seeking for employment. Check out the recent decision from India High Court on exonerated individuals and digital information.

Reflections

1. Does it work like this in Nigeria? Do we have a database to monitor convicted criminals and their activities?
2. Do you think this is a model that should apply to criminal convictions in Nigeria?
3. Can the right to be forgotten be activated in data processed for public interest?
4. Ever heard of the concept of CONTENT-FILTERING?

LawDigits
Education | Research | Innovation

RTBF UNDER THE NIGERIAN LAW

Under the Nigeria law. The NDPA in **Section 34** provides that a data subject has a right to erasure without undue delay; **Section 34(2)** states that a data controller shall erase personal data without undue delay where -

i. **The personal data is no longer necessary in relation to the purposes for which it was collected or processed or;**

ii. The data controller has no other lawful basis to retain the personal data.

This section birthed the ARAKA v. ECART case.

Article 38 of the GAID provides that a data subject has the right to have his or her personal data erased if:

1. Personal data is no longer necessary for the purpose of collection and processing.
2. Processing consent is withdrawn.
3. The data subject objects to processing for direct marketing activities.
4. Where the data processing as constituted, is unlawful.
5. In compliance with a legal ruling or obligation

LET US PUSH FOR OUR COUNTRY, WE CAN CHANGE THE WORLD ONE DATA AT A TIME

The same law provides that this right to erasure is not absolute. It stipulates that the right to be forgotten will not be enforced if:

1. Data is being processed for the purposes of freedom of expression and information subject to Section 45.
2. Compliance with legal ruling or obligation
3. Public Interest or exercise of organisation's official authority
4. Public Health purposes
5. Preventive or Occupational Medicine
6. The data is important information that serves public interest, scientific research, historical research or statistical purposes.
7. Data is necessary to establish a legal defence.

This applies to all the data processors involved in the processing of that personal data. Also, the law says the right may not apply where public interest is being pursued by disclosure of the data to the general public provided that public interest can be established by the data controller. See **Article 38 (4)** GAID 2025.

Let us examine the practicality, the implementation issues and the recommendations. These will take only one page. We are almost done.

Another interesting read on the right to be forgotten is the **ONLINE ERASER LAW** applicable in California.

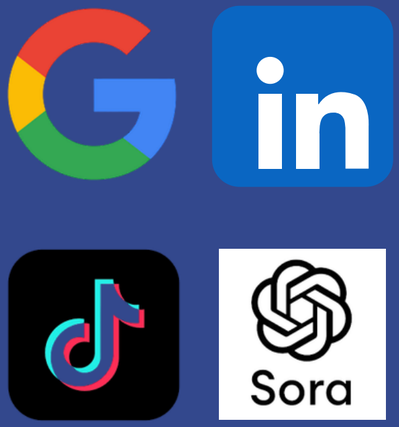
RTBF IN PRACTICE, OPERATIONAL CHALLENGES & RECOMMENDATIONS

The right to be forgotten is an enforceable privacy right recognised as expoused by both legislation and case law. The right can be enforced in different ways. Some of these ways include;

- Reporting to the Intermediary platform and requesting for an erasure. Some platforms have such options and if the claim is valid, it is removed after vetting. Usually, it is easier to go through the Nitda Code of Practice for Interactive Computer Service Platforms and Internet Intermediaries.
- Using a SNAG: Standard Notice to Address Grievance straight to the data controller.
- Report to the NDPC or FCCPC.
- You can go to Court.

Is this law being implemented in Nigeria? What is the rate of claims in the country? In July 2025, NITDA released their compliance report. In the report, Google reported that they received 951 complaints, Linkedin reported 10,134 and Tiktok reported 743,544. While these complaints may not entire be an exercise of a right to be forgotten, they represent the number of Nigerians that understand that they can consciously request to takedown about them or that are harmful. The operational challenges noticed include;

i. Data Controller Apathy within the country
ii Ultra-reliance on foreign service providers and infrastructure
iii. Enforcement speed and practices of the NDPC
iv. Widespread Ignorance of Data Subjects
v. Artificial Intelligence and the scourge of GenerativeAI



To fix these,
i. More sensitization of data controllers and data subjects
ii. Stakeholder engagements by regulator
iii. Sector by sector enforcement by the regulator

EQUIBRIDGE ATTORNEYS

BARRISTERS | CONSULTANTS | SOLICITORS

Hoping to participate in data protection civil class actions or file data privacy claims against your data controller? Reach out to us in **EBA** at **ebafirm@gmail.com**.

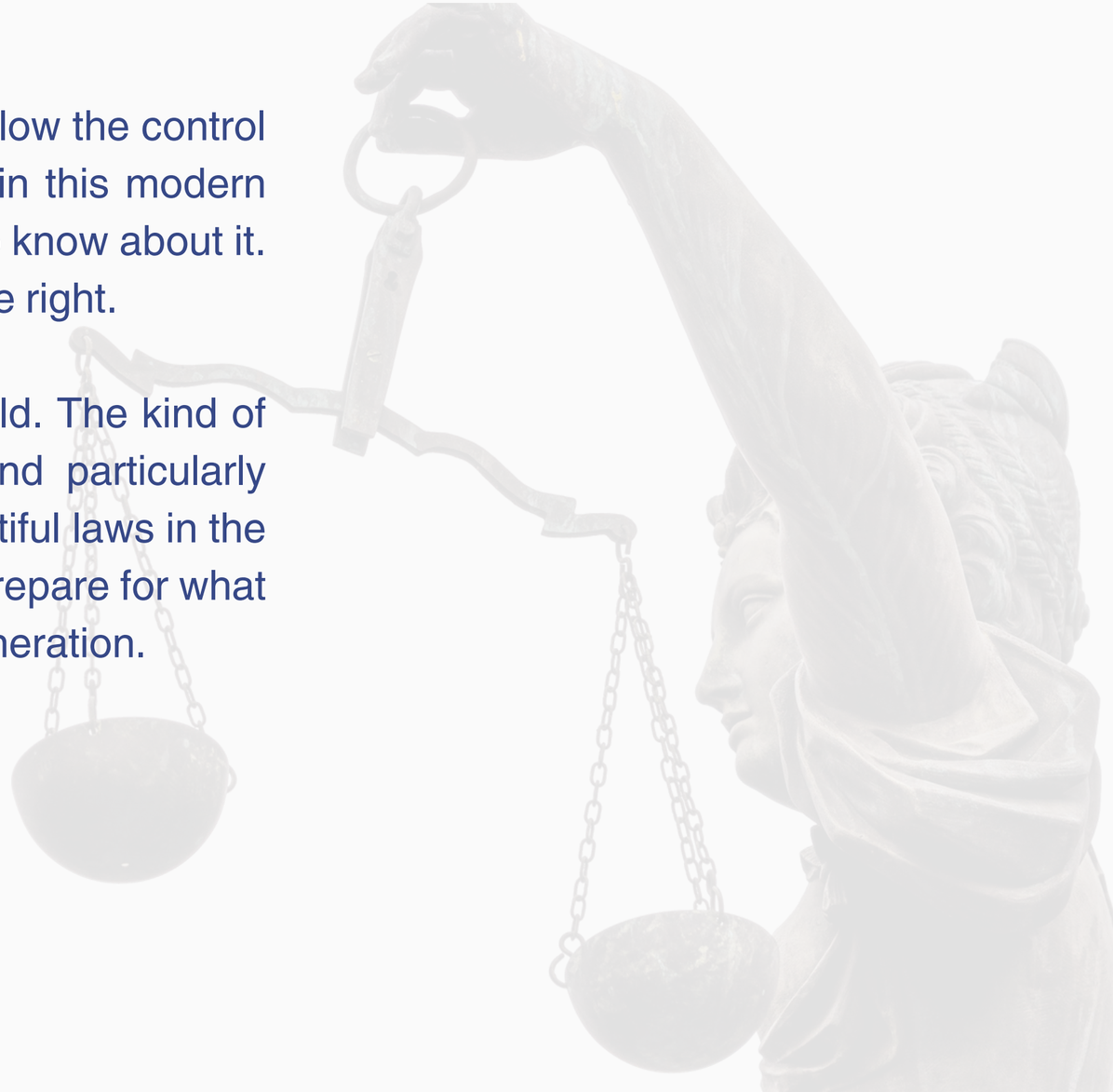
To know more about us, visit our website at: **www.ebafirm.com**

Follow us on LinkedIn

CONCLUSION

The right to be forgotten is one of the major rights to actually allow the control of the flow of personal data. The right has been established in this modern times. The major issue for Nigeria is how to get the populace to know about it. Also, when they know, how to make sure they do not misuse the right.

The fact remains that the law have evolved all around the world. The kind of laws humans have created in recent years are idealistic and particularly exigent for the technology age. We can only expect more beautiful laws in the future especially now that Artificial Intelligence is here. Let us prepare for what is to come. It will be a very interesting existence for our own generation.



Special Appreciation

LawDigits
Education | Research | Innovation

DATA PRIVACY
LAWYERS
Association of Nigeria

Hoping to be part of more conversations on how to address privacy, technology, cybersecurity issues and the sensitisation of executives and the entire population in Nigeria and beyond.

Thank you for the opportunity.

Most grateful.

DIPO IGE
Managing Partner, **EBA**
Convener, **LawDigits**
Director, Policy & Advocacy **(DPLAN)**