Special Issue on Data, Law and Decolonisation

Technology and Regulation

Is the Brussels Effect Creating a New Legal Order in Africa, Latin America and the Caribbean?

Dr. Patricia Boshe and Carolina Goberna Caride

Data Protection
Brussels Effect
Africa
Latin America and Caribbean

patricia.boshe@uni.pasau.de

Carolina.GobernaCaride@uni-passau.de

EU Regulation 2016/679 (GDPR), like the pied piper of Hamelin, has and continues to lure third countries into approximating the EU data protection framework. Some scholars believe the approximation of the EU framework, mostly done in a one-size-fits-all fashion, may not be appropriate in non-EU contexts mainly because (some) values advanced by the EU data protection framework may vary from or be incompatible with legal cultures and/or social norms of the recipient country/region. This paper looks into data protection in Africa, Latin America and the Caribbean (hereinafter LAC). The focus is on the evolution, influence and role of the EU in the development of data protection laws in Africa and LAC. The purpose is to ascertain whether and to what extent those laws are a result of the Brussels effect.

1. Introduction

Brussels is where the EU legislator resides and where norms with global impact, such as the EU Regulation 2016/679 (GDPR),[1] are drafted, hence the *Brussels effect* connotation. Simply put, the *Brussels effect* is Europe's assertion of 'unilateral power to regulate global markets' through 'legal institutions and standards.'[2] This unilateral regulatory globalization[3] acts as a gatekeeper in the global digital economy. For one, foreign countries and companies find themselves in a position where they have to comply with EU regulatory standards to participate in the EU internal market.[4] Data protection law is one of the strongest examples of the *Brussels effect*. In its 2018 annual report, the Mauritius Data Protection Commission noted the immense impact the GDPR has on its office. The report states, 'GDPR is regularly called upon to ensure that alongside compliance and enforcement under DPA, the GDPR is also being respected in its fundamentals, in order to avoid any situation where the reputation of Mauritius as a safe and democratic country respecting the basic human rights of people including the right to privacy, is not put at stake.'[5] According to this report, Mauritius had to amend its 2004 Data Protection Act in 2018 'in order to strengthen the control and personal autonomy of individuals over their personal Data and to comply in a timely way with the requirements of the General Data Protection Regulation (GDPR).'[6] The outreach of the GDPR is also seen in the Nigeria, where the Data Protection Implementing Regulation provides categorically that, 'Where the NDPR and this Framework do not provide for a data protection principle or process... European Union General Data Protection Regulation (EU GDPR) and its judicial interpretations shall be of persuasive effect in Nigeria.'[7] The Regulation goes further in declaring that through the GDPR, all EU and European Economic Area Countries are deemed to have adequate level of protection.[8] The annexure makes a substantive reference the GDPR and serves as a yardstick in determining which countries provide adequate data protection. Speaking on the experience of the U.S.A. in data protection regulation, Bradford illustrates how businesses are adjusting their practices to align with European legislative requirements.[9] She argues that the technical and economic non-divisibility of EU norms has forced companies such as Google, Apple, Airbnb, Uber and Netflix to modify their global privacy policies to comply with EU standards.[10]

1 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), OJ 2016 L 119/1.
2 Anu Bradford, 'The Brussels Effect' (2012) 107 Nw UL Rev 1..
3 Anu Bradford, 'The Brussels effect' (2012) 107 Nw UL Rev1, 3.
4 Id, 5.
5 Data Protection Office, *Annual Report January to December 2018* (10th Edition 2019), p. 5.
6 Id. 7.
7 Regulation 16 on p. 20-30.
8 See annexure C of the Nigeria Data Protection Implementing Regulation.
9 Anu Bradford, *The Brussels effect: How the European Union rules the world* (Oxford University Press 2020), 140.
10 Anu Bradford, *The Brussels effect: How the European Union rules the world* (Oxford University Press 2020), 143-144.

University of Passau (Both authors)

Between 2017-2018, Prof. Greenleaf conducted an assessment of about 132 countries with data protection laws.[11] He observed that the laws reflect in many ways provisions in the EU framework for data protection, the Data Protection Directive of 1995 and the GDPR.[12] In 2021, Greenleaf published a global table of data protection laws and bills. At the time, a total of 145 countries had adopted data protection laws.[13] His analysis of these laws and bills showed a strong influence of the GDPR and the Convention 108/108+[14] – a phenomenon also reflected in regions such as Africa,[15] as well as Latin America and the Caribbean (LAC).[16] The paper provides a thorough review of the history and the development of data protection in Africa and LAC. The objective is the see if, and to what extent far data protection in these regions are a result of the *Brussels effect*. The paper thus also analyses the challenges of implementing a law in new or foreign socio-cultural settings. The paper chose to focus on Africa and LAC as these regions have a more or less similar cultural setting, i.e communal societies, and less aggressive in asserting regulatory domination beyond their respective regions – unlike, for example, the EU, U.S, or China.

2. Development of Data Protection in the African Region and LAC

The history in the development of data protection legal frameworks in Africa and LAC differ. Prior to 2001, Africa, which consists of 55 nations (54 members of the African Union), had no comprehensive data protection framework. In addition, the right to privacy (which is closely tied to data protection) is not provided in the African Union Charter on Human and Peoples' Rights (hereinafter 'the Banjul Charter').[17] However, the right to privacy is incorporated in almost all African countries' constitutions.[18] Data protection regulation was introduced for the first time in 2001, when Cape Verde adopted a comprehensive data protection framework.[19] At the regional level, the African Union (hereinafter 'the AU') adopted the African Union Convention on Cyber Security and Personal Data Protection (hereinafter 'the Malabo Convention')[20] in 2014. The Malabo Convention came into force in June 2023 after attaining sufficient signature and ratifications from Member States.[21] – This is nine years after its adoption by the African Union. However, in June 2022, the AU published a tender for the review of the Malabo Convention.[22] The review is intended to align the Malabo Convention with technological developments and related risks to personal Data. In February 2022, the AU adopted the African Union Data Policy Framework (The Framework). The Framework presents a holistic approach to data regulation/governance. The Framework provides a governance structure for personal and non-personal Data. In terms of personal Data protection, the Framework adopts the seven data protection principles found in most data protection laws, i.e., 'consent and legitimacy; limitations on collection; purpose specification; use limitation; data quality; security safeguards; openness (which includes incident reporting, an important correlation to cybersecurity and cybercrime imperatives); accountability; and data specificity.'[23] The Framework, unlike the Malabo Convention, focuses on promoting digital transformation in Africa. Data governance and harmonization of related legal frameworks is seen as one of the main pillars to that end.

African states continue to adopt and review their legal frameworks. As of May 2023, 42 out of 54 African countries had comprehensive data protection frameworks[24] or bills/draft bills being discussed.[25] About eight African countries have reviewed or are in the process of reviewing their pre-GDPR laws to align with the GDPR.[26] This development is attributed to the inertia of the Directive 95/46/EC's adequacy requirement[27] and subsequently the GDPR.[28] Amidst this development, the Banjul Charter excludes the right to privacy from the catalogue of human rights. Scholars argue that African social values and legal culture lack emphasis on 'individual-based rights', which is why the Banjul Charter excluded the right to privacy.[29] Indeed, the Banjul Charter lacks any reference to the right to privacy. In addition, individual rights are structured in a way that gives the community or family an upper hand.[30] In this regard, the Charter states, it 'seeks not

11 Graham Greenleaf, 'Global Data Privacy Laws 2019: 132 National Laws & Many Bills' (2019) 157 Privacy Laws & Business International Report.
12 Id.
13 Graham Greenleaf, 'Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance' (2021) 169 Privacy Laws & Business International Report.
14 Graham Greenleaf, 'Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance' (2021) 169 Privacy Laws & Business International Report.
15 Patricia Boshe, Moritz Hennemann, Ricarda von Meding, 'African Data Protection Laws - Current Regulatory Approaches, Policy, and the Way Forward', (2022) Global Privacy Law Review.
16 Eduardo Bertoni, 'Convention 108 and the GDPR: Trends and perspectives in Latin America' (2021) 40 *Comput. Law Secur. Rev*, 3.
17 Adopted June 27, 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force Oct. 21, 1986.
18 See Patricia Boshe, Moritz Hennemann, Ricarda von Meding, 'African Data Protection Laws - Current Regulatory Approaches, Policy, and the Way Forward', (2022) Global Privacy Law Review.
19 Law No. 133-V-2001 on the Protection of Personal Data.
20 African Union Convention on Cyber Security and Personal Data Protection, adopted on the 27th June 2014 in Malabo, Equatorial Guinea.
21 According to Article 36 of the Malabo Convention, for it to come into operation, it required 15 ratifications from Member States. Upon the 15th ratification, the Convention will take effect 30 days after the last ratification.
22 The call for consultants can be found at the African Union Website.
23 The African Union, AU Data Plicy Framework, endorsed by the Executive Council during its 40th Ordinary Session held on 2 – 3 February 2022 through Decision with reference EX.CL/ Dec.1144(XL). Addis Ababa, February 2022, p. 51.
24 Algeria, Angola, Benin, Botswana, Burkina Faso, Cape Verde, Chad, Congo Brazaville (Republic of Congo), Cote d'Ivoire, Egypt, Gabon, Ghana, Guinea (Conakry), Kenya, Kingdom of Swaziland (eSwatini), Lesotho, Madagascar, Mali, Mauritania, Mauritius, Morocco, Niger, Nigeria, Rwanda, São Tomé and Principe, Senegal, Seychelles, South Africa, Tanzania, Togo, Tunisia, Uganda, Zambia and Zimbabwe.
25 Gambia, Malawi, Namibia, Nigeria (a federal comprehensive Act), and South Sudan.
26 Cape Verde (Law of 2001, amended in 2013 and in 2021), Burkina Faso (Law of 2004, under revision), Mauritius (Law of 2004, amended in 2017), Tunisia (Law of 2004, under revision), Senegal (Law of 2008, under revision), Benin (Law of 2009, amended in 2017), Morocco (Law of 2009, under revision), Mali (Law of 2013, amended in 2017). Cf. Patricia Boshe, Moritz Hennemann, Ricarda von Meding, 'African Data Protection Laws - Current Regulatory Approaches, Policy, and the Way Forward', (2022) Global Privacy Law Review.
27 Id; Alex Makulilo, '"One Size Fits All": Does Europe Impose its Data Protection Regime on Africa?' (2013) 447 Datenschutz und Datensicherheit, 450; Graham Greenleaf and Cottier, 'Comparing African Data Privacy Laws: International, African and Regional Commitments' (2020) University of New South Wales Law Research Series, 26.
28 Alex Makulilo, 'The Long Arm of GDPR in Africa: Reflection on Data Privacy Law Reform and Practice in Mauritius' (2021) 117 International Journal of Human Rights 127; Graham Greenleaf and Bertil Cottier, 'Data Privacy Laws and Bills: Growth in Africa, GDPR Influence' (2018) 152 Privacy Laws & Business International Report 11.
29 See for example Lee A Bygrave 'Privacy Protection in a Global Context: A Comparative Overview' (2004) *Scandinavian Studies in Law* 343; and HN Olinger et al 'Western Privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming Data Privacy Bill in South Africa' (2007) 39 *International Information & Library Review* 35.
30 See Article 9, 27 (2) of the Charter requiring an individual "to pay due regard to the rights of others, collective security, morality and common interest before they exercise their individual rights.

to isolate man from society but as well that society must not swallow the individual.' It is clear from this statement that individual rights are recognised under the Charter, but the role of the society in the enforcement of individual rights is acknowledged and overly emphasised. This approach is quite different from the approach of individualised communities.

African societies are communal societies and therefore, 'the idea of an individual as a right bearer is out of ordinary order.'[31] The arguments are strengthened by the fact that the Banjul Charter promotes the idea of a family and community as custodians of individual rights.[32] The Malabo Convention also emphasizes this premise. On Chapter II: Art. 8 (2) requires member states to ensure they recognize "prerogatives of the State, rights of local communities and purposes for which businesses were established" alongside the protection of personal data. This requirement is not reflected in the data protection laws adopted thus far in the region.

The Malabo Convention also emphasizes the need to resolve disputes amicably between parties/countries. If such an approach fails, the parties are to look for other peaceful means through mediation and conciliation boards and the like.[33] This approach reiterates the customary approach to dispute resolution in African communities – a system that encourages mediation and reconciliation. It discourages confrontation between parties and does not pronounce a winner or a loser in a dispute. It is a system of compromise where a winner wins a little and a loser loses a little.[34]

The history of privacy and data protection in the 33 LAC countries[35] is different from that of the African region. The Organization of American States (hereinafter 'OAS') adopted the American Declaration of the Rights and Duties of Man (hereinafter the American Declaration) in 1948.[36] This is the first (in the world) human rights instrument of general application, predating the Universal Declaration of Human Rights. Notice the difference in the titles between the American Declaration and the Banjul Charter. The latter speaks of 'peoples' rights' while the former speaks of 'rights of Man'. The Banjul Charter's title declares the plurality in its human rights system. On the contrary, the American Declaration insists on promoting an individual and his personality.[37] At the same time, the American Declaration recognizes the role of a community to an individual and that an individual has a duty to his community and nation; duties that are considered 'a prerequisite to the rights of all.'[38] This duty requires an individual to exercise his rights in relative rights of the society.[39]

Another difference from the Banjul Charter is that the American Declaration provides for the right to privacy. Individual privacy, privacy of a family,[40] privacy of one's dwelling[41] and his correspondences[42] are explicitly protected. The American Convention on Human Rights (Pact of San José) further reinforces these rights.[43]

Specifically, on the protection of personal data, LAC countries were the first (before the EU Directive 1995) to have a framework for the protection of personal data. This was in the form of a constitutional right known as *habeas data*. A constitutional writ roughly translated to mean *bring my data*. It takes a similar approach to the German right to self-determination[44] by giving citizens the right to access personal data and challenge their processing, and to correct or request deletion of such data.[45] *Habeas data* emerged as an emancipation tool in response to injustices and sufferings in the hands of military regimes (such as forced disappearances and extrajudicial executions). The objective was 'to assist family members looking for their missing loved ones'[46] and to guard against any recurrence of those.[47] It became a relevant tool for freedom of information challenging government misappropriation of personal data. *Habeas data* was later enacted into constitutions as a constitutional right.[48]

In 1999, Chile became the first LAC state to adopt a comprehensive data protection law.[49] By 2016, when the EU adopted the GDPR, 14 out of 33 LAC countries had comprehensive data protection laws.[50] In 2022, six years after the adoption of the GDPR, an additional seven

31 Patricia Boshe, Moritz Hennemann, Ricarda von Meding, 'African Data Protection Laws - Current Regulatory Approaches, Policy, and the Way Forward', (2022) Global Privacy Law Review.
32 Cf. Art. 18 (1) (2) and Art. 29 Banjul Charter. See also, Boshe, Hennemann and von Meding (n 15).
33 Article 34 of the Malabo Convention.
34 Patricia Boshe, Moritz Hennemann, Ricarda von Meding, 'African Data Protection Laws - Current Regulatory Approaches, Policy, and the Way Forward', (2022) Global Privacy Law Review.
35 UN ECLAC, https://www.cepal.org/en/estados-miembros ; https://www.un.org/en/about-us/member-states.
36 Adopted by the Ninth International Conference of American States, Bogotá, Colombia, 1948.
37 See paragraph one and two of the preliminary statements to the Declaration.
38 The paragraph two to the preamble of the American Declaration.
39 Article xxix of the American Declaration.
40 Article v of the American Declaration.
41 Article ix of the American Declaration.
42 Article x of the American Declaration.
43 The Convention was adopted in San José, Costa Rica on 22 November 1969 and came into force on 18 July 1978. See Article 11 on the right to privacy.
44 In Germany, information self-determination was declared a basic right in 1983 by the Constitutional Court in a census case. This right allowed an individual to exercise data rights such as access and deletion.
45 Based on the Resolution by the Supreme Court in Manila on the Rule on the Writ of Habeas Data, A. M. No. 08-1-16-SC (2008) - "Habeas Data is a remedy available to any person whose right to privacy in life, liberty or security is violated or threatened by an unlawful act or omission of a public official or employee, or of a private individual or entity engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence of the aggrieved party". See https://www.chanrobles.com/writofhabeasdata.html accessed on 02.05.2022.
"The Habeas Data does not require data processors to ensure the protection of personal data processed. It is presented as a legal action requiring the person aggrieved, after filing a complaint with the justice, the access and/or rectification to any personal data who may jeopardize their right to privacy." See http://www.oas.org/dil/data_protection_privacy_habeas_data.htm accessed on 02.05.2022.
See also, Lode, Sarah L. '"You Have the Data"...The Writ of Habeas Data and Other Data Protection Rights: Is the United States Falling Behind?," (2019) 94 Indiana Law Journal 41 p. 43 and Kati Suominen, 'Access to Information in Latin America and the Caribbean' (2003) 2 Comparative Media Law Journal, p. 31.
46 Sarah L Lode, "You Have the Data: The Writ of Habeas Data and Other Data Protection Rights: Is the United States Falling Behind" (2018) 94 Ind LJ Supp 41, 43.
47 Marc Tizoc González, "Habeas Data: Comparative Constitutional Intervention for Latin America against Neo-liberal States of Insecurity and Surveillance" (2015) 90 Chicago Kent Law Review 641, 642.
48 Some of the first countries to incorporate the writ of *habeas data* include Guatemala (1985), Nicaragua (1987) and Brazil (1988).
49 Law 19.628.
50 Chile (1999); Argentina (2000); Bahamas (2003); Saint Vicent and the Grenadine (2003); Uruguay (2008); Mexico (2010); Peru (2011); Costa Rica (2011); Trinidad and Tobago (2011); Saint Lucia (2011); Colombia (2012); Nicaragua (2012); Antigua and Barbuda (2013) and Dominican-Republic (2013).

countries had adopted comprehensive data protection laws,[51] five had pre-GDPR laws to align them with the GDPR,[52] four were reviewing their laws (possibly to align with the GDPR)[53] and seven countries were in the process of adopting comprehensive data protection laws for first the time.[54] In addition, in 2020, Brazil followed the EU by pronouncing data protection as an autonomous fundamental human right, separate from the right to privacy.[55] This was followed by an amendment of the Constitution to include data protection as a fundamental right.[56] Other LAC countries followed suit, with Nicaragua[57] including the right in Article 3(a) of its Data Protection Law 787, El Salvador whose Constitutional Court highlighted the legal certainty of the right,[58] and Costa Rica, whose Constitutional Court referred to the replacement of the classical concept of privacy with that of informational self-determination.[59] Moreover, before 2020 Argentina and Uruguay had already updated their data protection laws and acquired an adequacy decision.[60]

It is important to note that in 2017, the Ibero-America Data Protection Network adopted Standards for the Protection of Personal Data (hereinafter 'Standard Protection'). The purpose of the Standard Protection was to harmonize data protection legislative activities and create a common framework for the protection of personal data. It considered the GDPR as a benchmark (see preamble 8 of the Standard Protection).

3. Brussels Effect, Regulatory Convergence or Regulatory Acculturation[61]?

As already explained above in the introduction, the *Brussels effect* is attributed to the restriction on cross-border data flows and the extra-territorial overreach of Article 3 of the GDPR.[62] Eventually, 'forcing' legal assimilation in third countries including Africa and LAC. According to Christopher Kuner, third countries have little to no option but to assimilate the EU data protection framework to sustain cross-border data flows[63] and maintain international trade.[64] The fact that EU standards must remain applicable for data flows to take place[65] makes the EU framework highly competitive against other privacy and data-protection frameworks such as the U.S. and Asia. This is despite strong trade relations between Asia and the U.S. with Africa and Latin America.[66] This is best illustrated in the case of Bloggers Association of Kenya (BAKE) v Attorney General & 5 others, decided in Kenya in 2018.[67] In paragraph 11, it was argued, 'the implications of the coming into force of the General Data Protection Regulations (GDPR) on the 25th May 2018, which despite being European Union legislation, applies to all enterprises doing business with the European Economic Area regardless of location, and consequently the GDPR has extra-territorial effect. The implication is that in light of the conservatory orders granted herein, public and private Kenyan citizens remain exposed for failure to comply with the GDPR requirements to adequately protect data belonging to the European Union.' Eventually, in 2019, Kenya passed a Data Protection Act, the structure and contents of which closely resemble the GDPR. The fact that courts also took cognizance of Paragraph 254 in the case of Okiya Omtatah Okoiti & 4 others v Attorney General & 4 others; Council of Governors & 4 others (Interested Parties),[68] it is stated, '[t]he Data Protection Act No 24 of 2019 has adopted at section 2 the definition of personal data that is in the European Union's General Data Protection Regulations (GDPR), namely, any information which is related to an identified or identifiable natural person'. The GDPR continues to guide not only legal developments but courts' interpretations[69] beyond EU.

Still, caution should be taken; as already noted by the EU Data Protection Supervisor Mr. Wojciech Wiewioroski, the GDPR 'was drafted with the European Union in mind and as such it was never going to be a panacea to be copied and pasted to all jurisdictions worldwide.'[70]An argument supported by Daniel Berkowitz who insists that the EU framework is designed for the EU socioeconomic context and is informed by decades of iteration and discussions on the needs of Europeans parallel to their development stage. The fact also is evidenced by the shift from the Directive to the GDPR.[71] Nevertheless,

51 Barbados (2019); Panama (2019); Brazil (2020); Jamaica (2020); Belize (2021); Colombia (2021) and Ecuador (2021).
52 Brazil (2020); Trinidad and Tobago (2020); Uruguay (2020); Belize (2021); and Colombia (2021).
53 Argentina, Barbados, Chile and Costa Rica.
54 Bolivia, Cuba, El Salvador, Guatemala, Honduras, Paraguay and Suriname.
55 Direct Action of Unconstitutionality 6387, 6388, 6390 and 6393, Federal Council of the Brazilian Bar Association, Brazilian Social Democracy Party, Brazilian Socialist Party, Socialism and Liberty Party, Communist Party of Brazil v. Federal Government - Provisional Measure n. 954/2020, DJe. May 7th, 2020.
56 Action of 17 March 2022, the constitutional amendment (n°115) was enacted the 10th Feb. 2022 and then published in the official diary on 11 February 2022) Portal da Câmara dos Deputados (camara.leg.br).
57 May Rubby Pérez Martínez 'Protección de datos personales y derecho a la autodeterminación informativa: Régimen jurídico' (2020) 28 Revista de Derecho 107,122.
58 Judgment No. 934-2007, 4 March 2011, Constitutional Chamber of the Supreme Court of Justice, El Salvador (Sentencia No. 934-2007, del 4 de marzo de 2011).
59 Judgment No. 06484 of 10 May 2013, Constitutional Chamber of the Supreme Court of Justiceof Costa Rica (Sentencia N° 06484, de 10 de mayo de 2013).
60 Argentina (Decision 2003/490/EC); Uruguay (Decision 2012/484/EU).
61 Regulatory acculturation is described by Lee Bygrave as that which occurs when a state adopts the norms without significantly reflecting over their merits and does so because of various social pressures, such as maintaining membership in an "in-group" with a shared identity, or attaining social legitimacy. See Lee A. Bygrave, The "Strasbourg Effect" on data protection in light of the "Brussels Effect": Logic, mechanics and prospects 40 (2021) Computer Law & Security Review, 11.
62 Article 3(2) (a) and (b) of the GDPR has a direct application to third countries whenever goods or services are offered to European residents, profiling EU residents' behaviours, as long as the behaviour takes place with the EU. The provision gives the GDPR clear extraterritorial application. Additionally, Article 58 (1) (a) (b) of the GDPR empowers EU data protection authorities to conduct audit of data controllers and data processors in third countries. As a result of this audit, the EU data protection authority may suspend data flows to a recipient third country or an international organizations (see Article 58 (2)) (j) GDPR).
63 See also arguments by Christopher Kuner ,'The Internet and the Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (Oxford University Press 2019). 133.
64 Lee A. Bygrave, *Data Privacy Laws: An International Perspective* (Oxford University Press 2014). See also Lee A Bygrave 'Privacy Protection in a Global Context: A Comparative Overview' (2004) *Scandinavian Studies in Law* 343.
65 Christopher Kuner ,'The Internet and the Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (Oxford University Press 2019), 132.
66 Patricia Boshe, Moritz Hennemann, Ricarda von Meding, 'African Data Protection Laws - Current Regulatory Approaches, Policy, and the Way Forward', (2022) Global Privacy Law Review.
67 [2018] eKLR.
68 [2020] eKLR.
69 See for example the case of Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR.
70 Leaders League, *With the GDPR, Europe Shows the World the Way at* https://www.leadersleague.com/en/news/with-the-gdpr-europe-shows-the-world-the-way accessed on 10.11.2022.
71 Daniel Berkowitz et al., The Transplant Effect, 51 (2003) AM. J. COMP. L. 163, 168.

the 'exporting' of EU data protection values and standards seems to be EU's strategic move to ensure sufficient protection of its citizens.[72] So far, this strategic approach to protect personal data of EU citizens has led to the EU unilateral regulatory globalization.

Although China and the U.S are strong economic players in both Africa and LAC, their influence in legal development has yet to be seen.[73] Furthermore, the two countries do not yet have a strong hold on data protection regulatory environments (as compared to the EU) to influence or inspire other regions. China's data protection law is relatively new and the U.S. lacks a coherent data protection regime.[74] However, it is possible for either of the two countries to influence legal development in Africa or LAC in the future. More so for China, since "China and many African states share – *cum grano salis* – the notion of communalism as a social norm". This gives the strength over other frameworks, rendering it a 'golden standard' – to borrow the words of Viviane Reding.[75]

On the viability of a 'one-size-fits-all' legal framework, Finnemore and Sikkink have a contrary opinion. They argue that norms do not emerge from nowhere, but agents having 'strong notions about appropriate or desirable behaviour in their community' actively design them.[76] Peter Blume supports the above argument by writing about 'the way in which people think about law and legal issues. In a certain nation, there will be characteristic ways to conceive law and they may differ from the beliefs in another state. The formal instruments and institutions might be the same, but the differences in the culture imply that the law works or functions in different ways.'[77] A law or legal framework that disregards local culture would fail to provide solutions to local problems.[78] A living law is the one that is crafted to address local challenges and be responsive to domestic needs. This would mean the GDPR cannot and maybe should not be regarded as a framework suited for all purposes.

In addition, the need or motivation to create a certain legal framework may differ from one country/region to another. Histories, culture, and present social conditions (social, political, economic and technological) are determinants of a legal system. These aspects all together form a country's legal culture. This means a law should find a foundation to stand on in a specific community.

Blume adds, also 'some of the basic notions are not accepted everywhere'.[79] For example, the EU framework for data protection considers 'transparency', 'integrity', 'confidentiality', 'data minimization' and 'purpose limitation' as some of the core data protection principles. However, some African countries that adopted the EU framework 'omitted' some of the mentioned aspects from the list of basic data protection principles. Algeria, Egypt, Mauritania, are some of the countries whose data protection laws omitted 'transparency'. In Ghana, integrity and confidentiality are missing, and in Nigeria, data minimization and purpose limitation are missing. This would mean, even with the assimilation / importation of the EU data protection framework, the content might not be identical. In fact, expecting them to have identical rules across the globe would be unrealistic.[80] One cannot say with clarity that the omissions are intentional or a political or legal statement of some sort. But, looking at the pattern, for example, the omission of 'transparency' in more than three countries in one region, one can't help but wonder as to the motive behind such omissions.

In LAC, data protection frameworks (in the form of *habeas data*) preceded EU frameworks (both the EU Directive and the GDPR). In 2014, the Organization of American States (OAS) released the regional Statement of Principles for Privacy and Personal Data Protection in the Americas (SPPPDPA),[81] a model for data protection framework in LAC, which also preceded the GDPR. Such are the foundations that data protection law or frameworks can be built upon. It is, therefore, false to completely attribute the development of data protection regulation in LAC countries to the *Brussels effect*. Rather, it is a development consistent with existing and accepted norms in light of global (social, legal as well as technological) developments.

Habeas data as a framework to protect personal data became inadequate for its intended purpose. First, as a constitutional right, *habeas data* is limited to citizens or residents of a specific country. Hence, the protection is geographically limited. This framework would not support the nature of digital development and would hinder participation in the digital economy where personal data travels across borders. This would explain the adoption of comprehensive data protection frameworks by LAC countries to cover the protection loop left by *habeas data*.

The SPPPDPA reinforces the writ of *habeas data* as a central aspect in the protection of personal data, stating, 'the OAS principles reflect the concepts of informational self-determination, freedom from arbitrary restrictions on access to data, and protection of privacy, identity, dignity and reputation.'[82] This scope is wider than that of the GDPR. A data subject can enforce the writ of *habeas data* regardless of the data controller – such as the law enforcement or intelligence agencies – or the purpose of data processing – such as for national security or public order. This is not the case under the GDPR. Article 23 of the GDPR restricts data subjects' rights when the processing is by the aforesaid agencies or for the mentioned purposes.[83] In emphasizing this point,

72 See also European Commission, A European Strategy for Data, COM (2020) 66 final, 24.

73 Patricia Boshe, Moritz Hennemann, Ricarda von Meding, 'African Data Protection Laws - Current Regulatory Approaches, Policy, and the Way Forward', (2022) Global Privacy Law Review, 72.

74 Patricia Boshe, Moritz Hennemann, Ricarda von Meding, 'African Data Protection Laws - Current Regulatory Approaches, Policy, and the Way Forward', (2022) Global Privacy Law Review, 70.

75 Justice Commissioner Reding, who clearly emphasized the ambition for international norm promotion behind the regulation, stated during the drafting of the GDPR: 'Europe must act decisively to establish a robust data protection framework that can be the gold standard for the world. Otherwise, others will move first and impose their standards on us.'.

76 Finnemore and Sikkink International Organization at Fifty: Exploration and Contestation in the Study of World Politics (1998) 52 MIT Press 887, 896.

77 Peter Blume, 'Privacy as a Theoretical and Practical Concept' (1997) 11 International Review of Law Computers & Technology193, 194.

78 Justin Monsenepwo, "Decolonial Comparative Law and Legal Transplants in Africa" (2022) 121 ZVglRWiss, 168.

79 Peter Blume, 'Privacy as a Theoretical and Practical Concept' (1997) 11 International Review of Law Computers & Technology193, 68.

80 Alessandro Mantelero "The Future of Data Protection: Gold Standard vs. Global Standard" (2021) 40 *Computer Law & Security Review*.

81 At its 80th Regular Session in Mexico City in CJI/RES. 186 (LXXX-O/12) (March 2012).

82 At its 80th Regular Session in Mexico City in CJI/RES. 186 (LXXX-O/12) (March 2012).

83 Although in the EU there is a specific Directive regulating the process of personal data by intelligence and law enforcement agencies with - EU Directive 2019/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

the Constitutional Court in Dominican Republic ruled a GDPR-like data protection law as unconstitutional for restricting data subjects to exercise their rights on databases of the State's intelligence agencies, the rights that are guaranteed under Articles 44 and 70 of the Dominican Republic's Constitution.[84]

LAC countries, unlike Africa, have a long history of enforcing the right to privacy and data protection through the Inter-American Court of Human Rights (IACtHR).[85] In addition, like the EU, LAC countries recognize data protection as an autonomous fundamental human right. This is not the case in Africa. However, as Makulilo once argued,[86] this position is prone to change. As the world becomes 'smaller' due to globalization, culture and norms intermingle and hence change. He believes that, despite the prominence of communalism, individualism is emerging as a social value, 'suggesting the likelihood of replacing national values and cultures with cultural values of more technologically and economically advanced countries, particularly the United States and members of the European Union.[87]

Makulilo's observation may be demonstrated by the adoption of 'individual right-based' data protection frameworks adopted in Africa as a region, as well as in specific countries. However, this is not suggestive of the overall suitability of the GDPR in the region to justify a 'copy and paste' adoption. In fact, the Malabo Convention did not adopt the EU Directive in an exact one-size-fits-all approach. It made a few adjustments to support communal values and political situation/position in the regional human rights enforcement system. Article 8 of the Malabo Convention emphasizes the idea that individual data would be protected in cognizance of the communalistic nature of African societies and the role and rights governments have in enforcement of such rights. The Article states:

> 'The mechanism [for the protection of personal data] so established shall ensure that any form of data processing respects the fundamental freedoms and rights of natural persons while recognising the prerogative of the State, the rights of local communities and the purposes for which businesses were established.'

Additionally, the Malabo Convention encourages an alternative dispute resolution[88] versus a judicial way of dispute resolution. This again reflects an 'African' approach in dispute resolution – by encouraging negotiation and amicable settlement rather than seeking a winner and a loser in a conflict. This has been formalized in Kenya, where the Office of the Data Protection Commission (ODPC) designed a comprehensive Alternative Dispute Resolution Framework.[89] There are other divergences that could be interpreted as re-adjusting EU frameworks to local contexts. These include the class action system recommended by the Southern African Development Community (SADC) Model Law.[90] Swaziland (Eswatini) is an example of a country that endorsed the SADC approach. Section 50 of the Data Protection Act obliges the Data Protection Authority to create a system to deal with class actions.[91] In some countries, personal data are 'family property' whereby individual rights to personal data can be inherited.[92] Rwanda, South Africa and Nigeria are some examples of African countries whose data protection frameworks impose data localization obligations. Unlike the EU's GDPR, whose main goal is to facilitate free but secured flow of data within and beyond EU, data localization rules restrict the flow of data beyond local borders. These rules counteract the main purpose of developing data protection law, as stated in Article 1 (3) of the GDPR; '[t]he free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.'

The African region adopted a comprehensive data protection framework (Malabo Convention) in the absence of a foundation. Neither privacy nor data protection existed in the regional human rights charter. In fact, the two celebrated human rights are still not included in the catalogue of human rights within the Banjul Charter. This is quite different from the LAC and EU, where privacy has long been recognized as human right, and later, data protection as an autonomous fundamental human right. The primary human rights instrument in Africa, the Banjul Charter has declared neither the right to privacy nor data protection as human rights. Regardless, the AU and its member states continue to develop data protection laws following EU framework blue prints. EU influence on the development of data protection laws in Africa cannot simply be denied. Is it the Brussels effect that led to this development? I tend to lean towards Prof. Bygrave's argument that these laws are a 'response to protect threatened economies".[93] This argument is also supported by the fact that the laws 'have less emphasis on privacy and data protection as human rights rather as means to consumer confidence and overcoming trans-border data flow restrictions.[94]

4. Observations and conclusion

The appropriateness of any law or legal framework depends on its impact on basic societal values, its general acceptance within that specific society and the legal culture. Data protection systems affect both individuals and existing organizational (public and private) processing personal Data. On the one hand, individuals have an interest in protecting their Data, and on the other hand, organizations have an interest in controlling and processing personal Data. The latter aspect comes with the obligation to ensure the safety and integrity of personal Data. An additional interest comes from governments

84 Jiménez E M Marlen Court on the Personal Data Protection Law (Habeas Data Act) https://www.fundacionmicrofinanzasbbva.org/revistaprogreso/en/ruling-048416-from-the-constitutional-court-on-the-personal-data-protection-law-habeas-data-act/ accessed on 07.05.2022.

85 Souza et al. From Privacy to Data Protection: the Road ahead for the Inter-American System of Human Rights (2020) International Journal of Human Rights 147, 149 and 154. The right 'has appeared under different headings, as a right to be left alone, as a guarantee of personal development, of family life and a as part and parcel of the formation of individual opinion and thought within a democratic society.

86 Alex Makulilo 'The Context of Data Privacy in Africa' in Alex Makulilo (ed) *African Data Privacy Laws* (Springer 2016), 3.

87 Alex Makulilo 'The Context of Data Privacy in Africa' in Alex Makulilo (ed) *African Data Privacy Laws* (Springer 2016), 4.

88 Article 34 of the Malabo Convention.

89 https://www.odpc.go.ke/draft-alternative-dispute-resolution-framework-adr/.

90 Article 40 of the SADC Model Law.

91 Act No. 5 of 2022.

92 See for example Article 35 Algeria Data Protection Law (*Loi n° 18-07 Relative à la Protection des Personnes Physiques dans le Traitement des Données à Caractère Personnel)*;Article 63 of the Mauritania Data Protection Law (*Loi 2017-020 sur la Protection des Données à Caractère Personnel*); Article 25 in Rwanda Data Protection Law; and Articles 32 and 34 of the Tunisia Data Protection Law (*Loi Organique Numéro 63 en Date du 27 Juillet 2004 Portant sur la Protection des Données à Caractère Personnel*).

93 See Lee BygravePrivacy Protection in a Global Context: A Comparative Overview (2004) 47 Scandinavian Studies in Law, 343; Lee Bygrave Privacy and Data Protection in an International Perspective (2010) 56 Scandinavian Studies in Law, . 194.

94 Lee A. Bygrave, *Data Privacy Laws: An International Perspective* (Oxford University Press 2014), 76.

(political powers in place). More often, governments have an interest in Data ownership and in securing such Data. These varied interests in Data necessitate unique regulatory frameworks for Data protection that cannot easily be transplanted in a one-size-fits-all approach across cultures and communities.

We propose an inclusive approach in developing digital or Data protection laws, policies and regulation. Instead of one 'super legislator' or each region developing a framework in isolation and in disregard of the existence of other unique or different regulatory approaches. Digital economy and globalization necessitate coordinated and inclusive regulatory and policy decisions, regardless of whether the objective is to have a harmonized, converged or interoperable legal framework. To function in the globalised digital world, an all-inclusive rather than a one-size-fits all framework would be more fitting. As Tiberghien et al. once argued, 'no global, regional or national institution alone will be able to deliver the right governance capacity...some level of global coordination and basic rules for global co-existence are crucial.'[95]

95 Yves Tiberghien, Danielle Luo and Panthea Pourmalek *Existential gap: Digital/AI Acceleration and the Missing Global Governance Capacity* (Project for Peaceful Competition 2021) https://www.peaceful-competition.org/pub/85cu1r9n accessed on 09.05.2022.