Regulasi *Data Protection* untuk *Deceased Person*

Resha Puspita Dewi / 18217014

Mahasiswa, Institut Teknologi Bandung

ABSTRAK

Seiring dengan banyaknya aktivitas di dalam kehidupan sehari-hari yang ditranformasikan ke dunia digital, muncul berbagai kasus baru yang belum ada regulasinya. Benda-benda yang di dunia nyata tidak beridentitas, di dunia digital kini tercatat jejaknya. Identitas-identitas inilah yang tidak bisa dilepaskan begitu saja dari ranah hukum. Perlu adanya regulasi yang mengatur agar kepemilikan atas benda yang berwujud digital dapat dilindungi secara adil. Sebagian besar hukum telah dibuat dan diberlakukan bagi *living individuals.* Sedangkan, belum adanya kejelasan mengena regulasi yang ditujukan untuk *deceased.* Makalah ini membahas mengenai pengelolaan data di dunia digital dan regulasi terkait dunia digital yang diterapkan kepada *deceased*.

Kata Kunci: *deceased*, regulasi, *digital assets*

DAFTAR ISI

I. PENDAHULUAN

Perkembangan teknologi mengubah perilaku manusia secara perlahan. Hampir seluruh kegiatan manusia saat ini memanfaatkan keberadaan teknologi. Teknologi yang semula memudahkan manusia dengan kemampuan komputasinya, saat ini memudahkan manusia dengan adanya jaringan yang terhubung secara global. Jaringan ini telah membawa revolusi bagi perilaku manusia. Tidak hanya berkomunikasi secara jauh, jaringan ini juga dapat dimanfaatkan untuk mengendalikan benda-benda hanya dari satu perangkat *mobile*. Dari fenomena tersebut, tidak mengherankan jika aktivitas manusia akan lebih banyak dihabiskan di dalam jaringan.

Perubahan perilaku manusia yang mengikuti kemajuan teknologi menimbulkan tren baru di dunia digital. Perusahaan digital berinovasi untuk menjawab kebutuhan manusia yang bisa diotomatisasi menggunakan teknologi. Layanan-layanan dalam bentuk digital dihadirkan oleh perusahaan untuk kemudian digunakan oleh manusia dalam melakukan segenap aktivitasnya. Setiap aktivitas dalam jaringan ini tercatat dalam rekam jejak digital.

Sebagian besar kehidupan manusia yang telah ditransformasikan ke dalam bentuk digital membuat kita mengenal istilah identitas, kepemilikan, dan hak manusia dalam wujud digital. Diketahui bahwa ruang maya atau *cyberspace* tidak mengenal istilah *mortality*. Setelah penggunanya meninggal, sisa aktivitas pengguna yang berupa data tetap ‘hidup’ di dalam *cyberspace* [1]. Fakta ini yang kemudian menarik perhatian penulis terkait hubungan antara entitas manusia dengan kehidupan digitalnya. Manusia dikenal dengan siklus hidupnya yang dinamis atau tidak kekal. Bagaimana kehidupan digital menjanjikan perlindungan data bagi pengguna yang memiliki hak atas data yang masih tersimpan di dunia digital? Adakah segenap regulasi yang memberikan perlindungan data bagi pengguna yang telah meninggal?

Perlindungan data, khususnya yang berlaku pada *deceased person*, menjadi sebuah tantangan dalam dunia digital. Belum ada kajian yang spesifik membahas isu mengenai *data protection* bagi pengguna yang telah meninggal. Regulasi yang terkait dengan perlindungan data digital hanya berlaku untuk *living data subject*[1] atau subyek data yang masih hidup. Salah satu poin tujuan dibuatnya makalah kajian ini, yaitu untuk menggerakkan pihak-pihak yang mungkin terlibat dalam aktivitas pembuatan protokol perlindungan data agar mulai memberi perhatian lebih terhadap regulasi yang berlaku pada data digital bagi pengguna yang sudah meninggal.

[1] Seseorang yang dapat diidentifikasi melalui *identifier* berupa nama, nomor identitas, alamat atau *physical identifier* seperti genetik. (Definisi ‘*data subject*’ Art. 4 GDPR)

Pada bagian selanjutnya akan diuraikan beberapa bahasan yang dibagi menjadi 3 permasalahan sebagai berikut:

1. Bagaimana skenario pengelolaan data digital?
2. Bagaimana regulasi perlindungan data yang diterapkan pada pengguna yang telah meninggal?

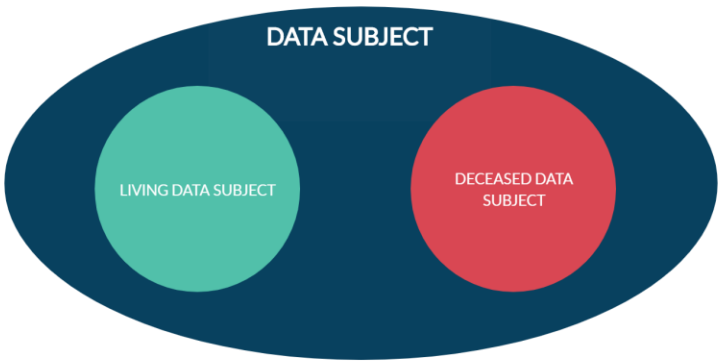
Adapun tujuan yang hendak dicapai dari pembuatan makalah kajian ini diuraikan menjadi poin-poin sebagai berikut:

1. Memberikan gambaran mengenai skenario yang terjadi berkenaan dengan penngelolaan data digital.
2. Membahas regulasi perlindungan data digital bagi *deceased*.

Penulis hendak membagi pembahasan menjadi 3 (tiga) bagian utama. Pada bagian pertama pembahasan, akan dimulai dari memahami pengelolaan data digital. Pada bagian tersebut akan dikenalkan mengenai berbagai istilah data yang akan digunakan sepanjang pembahasan, skenario pennyimpanan data, dan sisi keamanan data digital. Di bagian awal pembahasan yang selanjutnya akan dibahas mengenai kasus yang terjadi terkait penyalahgunaan data. Selanjutnya, analisis mengenai regulasi yang tepat untuk perlindungan data digital dengan objek pembahasan, yaitu pengguna yang telah meninggal. Pada bagian akhir makalah, penulis menyimpulkan hasil analisis yang ada pada bagian pembahasan.

II. PENGELOLAAN DATA DIGITAL

Di dunia digital, terdapat pendefinisian bagi nomina penduduk atau pengguna internet yang kemudian dikenal sebagai *data subject* atau *natural person.* Kedua istilah ini bisa digunakan secara bergantian. Namun, pada makalah ini kita akan lebih sering menggunakan penyebutan *data subject*, pengguna, dan *deceased* secara bergantian.



Gambar 1: Diagram Venn Data Subject

Untuk mempermudah pemahaman mengenai objek pembahasan, disajikan gambar sebuah diagram venn yang menunjukkan hubungan antara tiga komponen di dalam himpunan. Dari gambar diagram di atas, ditunjukkan bahwa *data subject* memiliki 2 kategori berbeda, yaitu *living data subject* dan *deceased data subject*. Di dalam makalah ini, akan banyak dibahas mengenai regulasi perlindungan data yang menyangkut *deceased data subject*. Di pendahuluan sebelumnya, telah dibahas mengenai istilah *living data subject*. Sepanjang pembahasan, pengguna internet yang telah meninggal akan disebut dengan istilah *deceased data subject*.

Pada pembahasan kali ini, akan diuraikan mengenai proses pengelolaan data digital secara umum sebelum memasuki pembahasan terkait klasifikasi dan regulasi perlindung data yang ditujukan kepada *deceases data subject*.

A. Skenario Penyimpanan Data Digital

Seiring dengan banyaknya aktivitas pengguna yang dilakukan melalui jaringan, banyak data yang tersimpan di dalam jaringan. Berbagai macam data tersebut bisa data-data yang kita simpan di akun Linkedin, riwayat pencarian kita di Google, koneksi kita di Facebook, aktivitas konsumtif kita di *e*-commerce, bahkan rekam medis yang hari ini sudah tersimpan secara *online.* Setelah kita membahas sedikit mengenai *data subject*, diketahui bahwa usia identitas digital dari suatu *data subject* hidup lebih lama dibandingkan dengan usia dari *data subject* itu sendiri. Ketika *data subject* dari suatu layanan digital meninggal, *data subject* tersebut meninggalkan konten dan data digital yang terakumulasi selama masa hidup mereka. Konten digital yang dimaksud, selain beberapa contoh yang sudah disebutkan sebelumnya, dapat berupa pesan di *email* atau YouTube *playlist*. Sepeninggal *data subject*, konten dan data digital tersebut masih tersimpan baik secara *online* maupun di gawai pengguna. Seluruh konten digital tersebut menjadi residu atau *digital remains*, yang merupakan potongan atau bagian yang merefleksikan kepribadian pengguna [2].

Jika dikategorikan ke dalam kelompok yang lebih kecil lagi, *digital remains* terbagi lagi ke dalam kelompok *tangible* dan *sentimental*.[2] Kedua kelompok *digital remains* tadi dapat dikategorikan sebagai *digital assests*. Karena pada dasarnya data *tangible* dapat berupa akun berbayar pengguna yang memiliki fitur premium. Sedangkan data *sentimental* merupakan data yang hampir keseluruhan riwayat aktivitas pengguna dapat dikelompokkan ke dalam data *sentimental*. Data-data inilah yang kita sebut juga sebagai *digital assests*,

[2] Istilah '*tangible'* dan '*sentimental*' mengikuti penyebutan yang ada di artikel Forbes.com ditulis oleh Bernard Marr (2017) *What Really Happens To Your Data After You Die?*

material utama yang menjadi objek regulasi dalam melakukan perlindungan data. Pada pembahasan terkait regulasi, kita akan lebih sering menggunakan istilah '*digital assets'* dibandingkan '*digital remains*'.

Digital remains yang ditinggalkan oleh pengguna tentunya tidak akan berarti apa-apa tanpa personifikasi dari data tersebut. Personifikasi data tersebut didapatkan dari beberapa *identifier*[3] yang menjadikan kumpulan data tersebut mengerucut ke suatu identitas pengguna. *General Data Protection Regulation* (GDPR), undang-undang yang mengatur tentang perlindungan data, mendefinisikan *personal data* sebagai kumpulan informasi yang dapat mengidentifikasi suatu individu. Sekumpulan informasi ini diklasifikasikan menjadi beberapa *identifier*. *Identifier* penting yang berperan memberikan *personal data* pengguna, di antaranya: nama, akun sosial media, *identification numbers* seperti NIK, data lokasi, dan data lainnya yang dapat menggambarkan kondisi fisik, psikologis, genetik, mental, ekonomi, sosial dan budaya pengguna [3]. Adanya *personal data* pengguna yang tercatat secara digital mengakibatkan *digital remains* bukan lagi sekadar residu yang keberadaanya tidak bernilai.

Barangkali, pengguna tidak secara sadar memberikan *personal data* mereka. Dunia digital memang telah membuatnya menjadi kasat mata. Setiap pengguna yang hendak menggunakan layanan digital, baik dalam jaringan ataupun tidak, akan diminta untuk mengisi beberapa data untuk dapat menggunakan layanan tersebut. Pengisian data ini disyaratkan oleh penyedia layanan sebagai kontrak bagi pengguna yang hendak memanfaatkan layanannya. Jadilah, melalui interaksi ini berbagai perusahaan penyedia layanan digital memiliki aset berupa data personal pengguna.

Dunia digital kini telah mengenal istilah *post-mortem privacy* sebagai solusi teknologi atas upaya perlindungan data. Di dalam bukunya, Harbinja [4] menjelaskan *post-mortem privacy* sebagai 'hak pengguna untuk melestarikan dan mengendalikan apa yang menjadi reputasi, martabat, integritas, rahasia atau ingatannya setelah mati'. Konsep tersebut telah menyiratkan bahwa pengguna pada dasarnya memiliki hak untuk membuat keputusan terkait pemrosesan data pribadinya setelah meninggal.

B. Sisi Keamanan Data Digital

Jika membahas sisi keamanan, medium data yang dapat diukur secara profesional ialah data yang tersimpan secara digital dan di dalam jaringan. Sebab, jarang terjadi kasus penggunaan data yang dilakukan oleh kerabat pengguna dijatuhi hukum, sekalipun

[3] pembeda, pengidentifikasi

penggunaan data tersebut dikategorikan sebagai cara yang ilegal. Perlu intruksi khusus dari pengguna apabila terjadi penyalahgunaan data digital yang terjadi secara *offline* yang dilakukan oleh kerabat pengguna. Untuk itu, sepanjang pembahasan ini kita akan fokus membahas hukum, regulasi, atau keamanan data digital yang terjadi di dalam jaringan.

Ada pertanyaan menarik yang dicetuskan oleh Bollmer di dalam artikelnya [5], yaitu "*What happens if the representation of the body as data, as detached from the body, is one in which death cannot be presented?*". Pertanyaan tersebut menggelitik pengguna internet untuk memikirkan tentang kelanjutan data milik pengguna setelah ia meninggal. Diungkapkan pula oleh Bollmer bahwa pemikiran ini telah mengantarkan kecemasan kepada pengguna. Fenomena kecemasan yang dirasakan pengguna bukan tanpa dasar. Faktanya, dari sekian banyak *social networking platform,* hanya segelintir yang menyediakan opsi bagi pengguna untuk mengatur akun mereka setelah meninggal. Sebagian besar *platform* jejaring sosial tidak memberikan fitur yang memadai kepada pengguna untuk mengimplementasikan rencana atau perlindungan data mereka setelah kematian. Kekurangan ini menjadikan data pengguna yang terdapat di dalam layanan rentan terhadap pelanggaran privasi dan penyalahgunaan [6].

Dijelaskan pula di dalam artikel OneZero [6] bahwa perusahaan sekelas Skype bahkan tidak (atau belum) memiliki *policy* untuk mengatur akun *deceased*. Perusahaan seperti Twitter, Instagram, dan Snapchat telah memberikan fitur berupa *flaaging* untuk menandakan akun *deceased* dengan konfirmasi dari anggota keluarga atau teman yang terpercaya. Adapun tujuan dari fitur *flagging* ini hanya sebatas untuk menghapus akun *deceased* dari saran pertemanan.

Sisi keamanan digital membutuhkan suatu kebijakan yang memungkinkan pengguna menunjuk orang kepercayaannya untuk menangani akun setelah pengguna. Perusahaan sekelas Google dan Facebook telah menyediakan opsi ini, yang disebut dengan *legacy contact*. Orang ini memiliki akses untuk *memorialize* profil pengguna setelah kematian atau menghapusnya secara permanen. Namun, kebijakan ini tidak menentukan lebih lanjut apa yang terjadi jika *legacy contact* ini telah meninggalkan layanan. Akun yang tidak dihapus atau diabadikan di dalam layanan membuat ia menjadi lebih mudah diretas. Sebab, akun yang ditinggalkan atau jarang digunakan tidak ada yang memeriksa sehingga lebih rentan terkena pencurian identitas, penipuan, dan disalahgunakan untuk merugikan orang lain [6].

Di dalam praktik dunia nyata, kita mengenal tradisi pemakaman untuk mengantarkan jenazah. Model praktik ini diharapkan juga diterapkan untuk data digital. Terdapat istilah *digital data funeral*, yaitu proses kremasi data bagi pengguna yang telah meninggal. Konsep ini bertujuan untuk memperkenalkan artefak digital untuk (secara konseptual) dimasukkan

dalam ritual pemakaman sebagai wujud dari eksistensi pengguna. Sebab, keseluruhan data pengguna yang telah tersebar di dalam jaringan dapat dianggap sebagai bentuk baru dari *hybrid memory* yang berhubungan dengan memori lokal manusia atau pengguna [7].

III. REGULASI PERLINDUNGAN DATA

Banyak hukum yang berlaku menyatakan bahwa *deceased* tidak memiliki hak di dalam hukum. Sebab, secara nalar *deceased* tidak dapat melakukan aktivitas, terlebih yang berkaitan dengan hukum. Aktivitas yang berkaitan dengan hukum tersebut ialah menikah, bercerai, atau menggugurkan hak pilih di dalam pemilu. Diketahui bahwa di dalam kasus urusan warisan, *deceased* menjadi pihak yang tidak dapat dituntut. Aturan pelaksanaan ini yang menyebabkan lemahnya perlindungan hak bagi *deceased*. Misalnya saja, *deceased* memiliki catatan medis sepeninggalnya. Catatan medis ini terkikis nilai privasinya sebab kematiannya telah memberikan anggota keluarga atau orang terdekat untuk dapat mengakses catatan medis miliknya. Meskipun begitu, diungkapkan bahwa telah banyak lembaga hukum yang memberikan perhatian lebih untuk melindungi hak-hak *deceased*. Timbal balik dari regulasi yang mengikat *deceased* tersebut adalah dilaksanakannya wasiat *deceased* sebagai hukum yang sah sekalipun bertentangan dengan preferensi orang hidup [8]. Pada makalah ini kita akan mengkaji lebih lanjut tentang perlindungan hak berupa perlindungan data digital yang ditinggalkan oleh *deceased*.

A. Kepemilikan Properti oleh *Deceased*

Banyak elemen yang dapat terlibat di dalam kasus data digital. Elemen-elemen tersebut di antaranya penyedia layanan, individu, atau bahkan individu penyedia layanan. Dengan mempelajari sejumlah kasus yang melemahkan perlindungan data digital, diharapkan mampu membantu upaya perumusan regulasi agar dapat ditinjau dengan lebih bijak. Sebab, selama regulasi perlindungan data *deceased* belum dapat meliputi semua permasalahan yang ada terkait *deceased,* maka selama itu pula *digital remains* yang ditinggalkan oleh *deceased* mengalami kerentanan.

Terdapat kasus yang cukup tenar di Jepang, dijelaskan oleh Profesor Ashir Ahmed, *Kyushu University*, tentang kasus penyalahgunaan data yang membidik penduduk Jepang. Disebutkan adanya beberapa keluarga di Jepang yang mendapatkan teror untuk membayar sejumlah tebusan kepada peneror. Peneror tersebut mengaku memiliki data *deceased* yang akan membahayakan reputasi keluarga tersebut jika data ini tersebar [6]. Kasus tersebut

menunjukkan adanya penyalahgunaan yang diakibatkan oleh, salah satunya, *deceased* itu sendiri. Penyalahgunaan ini disebabkan oleh karena tidak terencananya pengamanan data kepemilikan *deceased* sehingga memiliki celah untuk membahayakan kerabat atau orang yang ditinggalkannya.

Dikarenakan aktivitasnya di dalam dunia digital, pengguna memiliki *data assests* yang perlu dikelola. Untuk *digital assests* yang dimiliki *deceased*, terdapat opsi bagi orang kepercayaan *deceased* mengelola *digital assets* milik *deceased* sesuai dengan wasiat yang ditinggalkan *deceased.* Bagaimana nasib *digital assets* yang ditinggalkan oleh pengguna yang tidak meninggalkan wasiat? Di titik inilah peranan hukum diharapkan mampu mengimbangi perubahan teknologi. Sudah ada *Internet Service Provider* (ISP) yang menerapkan perlindungan data bagi *deceased.* Perlindungan ini berupa perlindungan *digital assets* milik *deceased* yang diperlakukan layaknya *physical property.*

Ketika seorang pengguna menggunakan layanan yang ada di internet, maka penyedia layanan akan menerapkan perlindungan bagi *digital assests* yang dimiliki oleh pengguna. Perusahaan atau penyedia layanan ini tidak akan memberikan informasi apa pun tanpa persetujuan pengguna yang telah menyepakati kontrak dengan penyedia layanan. Sekarang ini, pengguna dapat memilih *digital executor*[4] sebagai seseorang kepercayaan yang memegang *password* sosial media pengguna. *Digital executor* ini dapat diberikan kepercayaan untuk mengatur *digital assets* bagi pengguna yang telah meninggal. Beberapa yang masuk ke dalam contoh *digital assets* ialah akun media sosial, publikasi atau konten yang mengandung hak cipta oleh pengguna. *Digital assests* lainnya yang benar-benar memiliki value secara ekonomi yaitu akun yang bermitra dengan penyedia layanan dan mendapatkan keuntungan dari akun mitra tersebut. Contoh akun mitra yaitu akun YouTube yang sudah bisa dipasang iklan, akun mitra Quora yang mendapatkan royalti dari jumlah penayangan pertanyaan, dan akun media sosial lainnya yang menghasilkan pendapatan [9]. Sayangnya, keberadaan *digital executor* yang diharapkan dapat mengelola *digital assets* milik *deceased* sangat bergantung dengan hukum dimana *deceased* menetap.

B. Kontrak yang Disepakati oleh *Deceased*

Setiap kali pengguna internet hendak menggunakan layanan yang tersedia di internet, pengguna selalu diminta untuk menyetujui "*Term of* Service" yang diajukan oleh penyedia layanan. Persetujuan yang diberikan pengguna *sesederhana* pengguna meng-klik "*I agree..*"

[4] Istilah yang disadur dari artikel *tech culture* di IPerity.com

pada *checkbox* yang tersedia. Padahal justru di tahap ini pengguna telah memberi kewenangan yang serius kepada penyedia layanan untuk mengatur privasi milik pengguna. Persetujuan ini merupakan kontrak antara pengguna dengan penyedia lanyanan. Sayangnya, penyedia layanan membuat kontrak sesuai dengan *interest* mereka, perjanjian dibuat dengan tidak merugikan penyedia layanan [10]. Selain itu, tidak jarang suatu penyedia layanan melibatkan pihak ketiga yang membuat urusan kontrak ini menjadi lebih rumit. Hal ini dikhawatirkan apabila kontrak antara penyedia layanan dengan pengguna tidak cukup untuk meliputi perlindungan data bagi *deceased*.

Skenario perlindungan data untuk *deceased* umumnya bertolakbelakang dengan *term of service* yang ada. Umumnya, kontrak yang berlaku tidak memperkenankan pengguna untuk memberikan informasi *login* kepada orang lain. Hal ini menyebabkan kontrak dengan penyedia layanan dianggap sebagai penghalang atas wasiat *deceased* sebagai tindak lanjut dari pengunaan akun *deceased.* Dengan tidak adanya regulasi khusus yang berfungsi melindungi data *deceased* menyebabkan adanya kontradiksi antara keinginan *deceased* dengan t*erm of service* yang diakui secara hukum.

Hukum yang berlaku melakukan pendekatan dengan cara memberikan perlakuan yang sama antara *digital assets* dengan *physical property*. Sebagai mana perbedaan uang elektronik dengan uang fisik, keduanya tidak sama karena adanya identitas di dalam *digital assets,* sedangkan di dalam *physical property* tidak ada. *Digital assets* dianggap memiliki material untuk mengungkapkan keseluruhan informasi *deceased* [10].

C. Perlindungan Data Digital yang Telah Berlaku

Poin penting dari perlindungan data digital ialah permasalahan privasi. Dibawah undang-undang GDPR, pengguna memiliki hak untuk mendapatkan salinan data digital miliknya serta hak untuk menentukan data tersebut dihapus atau tidak.[5] Sayangnya, secara tegas, GDPR menyebutkan undang-undangnya hanya berlaku untuk *living data subject.*[6] Privasi yang diatur di dalam undang-undang ini meliputi data personal. Pasalnya, tidak semua konten pengguna di dalam internet merupakan data personal. Ada beberapa di antaranya yang merupakan hak intelektual yang diperlakukan sebagai *digital assets* [11].

Telah disebutkan [11] berbagai kebijakan perlindungan data bagi *deceased* yang telah berlaku di berbagai negara. Di Perancis, pengguna memiliki andil untuk menentukan apa yang akan diberlakukan pada data mereka setelah mereka meninggal. Di Canada, dikenal

[5] Aturan '*Right to erasure'* Art. 17 GDPR
[6] Aturan *'Not Applicable to Data of Deceased Persons'* Art. 27 GDPR

deceased's executor sebagai seseorang kepercayaan *deceased* yang akan mengelola *digital assets* milik *deceased.* Di Jerman, terdapat aturan yang menyamakan hukum surat wasiat dengan akun sosial media. Dengan adanya aturan ini, ahli waris diizinkan mendapat akses secara penuh data peninggalan *deceased.* Di Italia, disebutkan di dalam undang-undang mereka Pasal 9 (3), akses terhadap data *deceased* diizinkan untuk pihak yang memiliki *concern* terhadap data *deceased* atau sekadar alasan kekerabatan. Kebijakan yang berlaku di Amerika Serikat, berlaku hampir di seluruh negara, mengizinkan ahli waris untuk mengakses riwayat komunikasi *deceased* tetapi akses terhadap kontennya berlaku setelah mendapat izin di pengadilan.

IV. KESIMPULAN

Berbagai aktivitas pengguna di dalam internet menyisakan berbagai data yang, jika dilakukan *compiling* terhadap data, dapat mempresentasikan eksistensi pengguna. Perihal informasi personal, *cookie, tracking technologies* yang diterapkan kepada data pengguna dikelola oleh penyedia layanan dan disepakati oleh pengguna. Perlindungan Data bagi *deceased,* pengguna yang sudah meninggal, ditujukan untuk melindungi privasi yang dimiliki oleh *decased.* Sebagian besar data yang sensitif yang mengandung privasi bersumber dari akun-akun media sosial yang memiliki fitur obrolan.

Standarnya, d*eceased* tidak memiliki kendali atau hak di ranah hukum, termasuk hak *post-mortem privacy*. Namun, hukum kini telah melakukan upaya untuk menyeimbangkan hak antara *living indiduals* dengan *deceased.* Hal ini diwujudkan dalam perlindungan *digital assets* milik *deceased* yang derajatnya disamakan dengan hukum *physical* property. Persamaan hukum itu diberlakukan apabila tidak ada intruksi khusus dari *deceased* yang dituangkan dalam surat wasiat. Ada kalanya regulasi yang berlaku di ranah hukum dipandang lemah dalam melindungi hak *deceased.* Ketika terdapat kasus terkait *data remains* milik *deceased* yang tidak secara jelas diatur di dalam hukum, kasus tersebut diadili dengan *terms of service* yang telah disediakan penyedia layanan digital. Padahal diketahui bahwa *terms of service* ini lebih banyak melindungan hak dari penyedia layanan, bukan pengguna.

Salah satu alternatif yang dapat dimasukkan ke ranah hukum, yaitu dengan memperluas pendefinisian aset milik *deceased* sehingga *digital assets* mendapatkan payung hukum yang terstandardidasi. Derajat regulasi ini nantinya memiliki kedudukan yang lebih tinggi dibandingkan dengan *term of service* penyedia layanan. Alternatif lainnya, jika hanya mengandalkan kontrak dengan penyedia layanan, penyedia layanan perlu menambahkan opsi "*digital executor*" yang akan bertanggung jawab atas kepemilikan data *deceased.* Opsi *digital*

executor yang dimuat dalam kontrak antara pengguna dan penyedia layanan ini nantinya akan diakui di dalam hukum.

Referensi

[1] F. Hussain, M. Mostafa, and D. Usmonova, “Digital walking dead- How safe is the global south?,” *ACM Int. Conf. Proceeding Ser.*, vol. Part F1320, pp. 1–5, 2017, doi: 10.1145/3136560.3136593.

[2] M. Savin-Baden and V. Mason-Robbie, *Digital Afterlife: Death Matters in a Digital Age*. CRC Press, 2020.

[3] L. Ryz and L. Grest, “A new era in data protection,” *Comput. Fraud Secur.*, vol. 2016, no. 3, pp. 18–20, 2016, doi: 10.1016/S1361-3723(16)30028-8.

[4] E. Harbinja, “Post-mortem privacy 2.0: theory, law, and technology,” *Int. Rev. Law, Comput. Technol.*, vol. 31, no. 1, pp. 26–42, Jan. 2017, doi: 10.1080/13600869.2017.1275116.

[5] G. D. Bollmer, “Millions Now Living Will Never Die: Cultural Anxieties About the Afterlife of Information,” *Inf. Soc.*, vol. 29, no. 3, pp. 142–151, 2013, doi: 10.1080/01972243.2013.777297.

[6] C.-Y. Hou, “Data Thieves Are Targeting Dead People’s Social Media Accounts,” *Medium*, 2020. [Online]

[7] T. Kohn, M. Gibbs, B. Nansen, and L. van Ryn, *Residues of Death: Disposal Refigured*. Taylor & Francis, 2019.

[8] K. R. Smolensky, “Rights of the Dead,” *SSRN Electron. J.*, vol. 37, no. 3, 2011, doi: 10.2139/ssrn.924499.

[9] M. Bakhoum, B. C. Gallego, M. O. Mackenrodt, and G. Surblyt\.e-Namavičien\.e, *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* Springer Berlin Heidelberg, 2018.

[10] Natasha Chu, “Protecting Privacy After Death,” *Northwest. J. Technol. Intellect. Prop.*, vol. 13, no. 2, pp. 255–275, 2015.

[11] Thomson Reuters Foundation, “Data Ownership After Death is ‘A Complete Legal Mess,’” *The Japan Times*, 2019. [Online]