Konsensus : Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi
Volume 3, Nomor 3, Juni 2026
E-ISSN .: 3048-1325 ; P-ISSN .: 3048-440, Hal. 108-120
DOI: https://doi.org/10.62383/konsensus.v3i3.1770
Tersedia: https://journal.appisi.or.id/index.php/konsensus

Genomic Insecurity: Kebocoran Data *23andMe* dan Transformasi *Biosecurity* terhadap Identitas Genetik dalam Perspektif *Human Security*

Adinda Gladys Hartisya [1*], Imam Fadhil Nugraha [2]
[1,2] Departemen Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin, Indonesia

**Penulis Korespondensi: agladyshartisya@gmail.com*

Abstract. *This paper analyzes the genetic data breach experienced by the biotechnology company 23andMe in 2023 and its impact on individual security, focusing on the transformation of genetic data into an instrument of power within the framework of non-traditional security threats. Using a descriptive analytical method based on a literature review, this paper explores three main dimensions; the credential stuffing attack mechanism that exploited the DNA Relatives feature, thereby exposing millions of user accounts globally; the operationalization of corporate biopower through the Direct-to-Consumer model that positions 23andMe as a non-state biological administrator, and the relational and hereditary nature of genetic data that extends the threat to family networks and future generations. These are analyzed through the integration of Michel Foucault's biopolitical theory and human security, with the dimension of health security serving as the primary analytical framework. Therefore, this paper demonstrates that the 23andMe data breach is not merely a technical cyber failure, but rather a manifestation of the shift in the logic of bio-surveillance from state authorities to the realm of commercial corporations, creating permanent, systemic, and unequal vulnerabilities.*

Keywords: *Biopolitics; Data Breach; Genetic Data; Human Security; Non-Traditional Security.*

Abstrak. Tulisan ini menganalisis kebocoran data genetik yang dialami perusahaan bioteknologi *23andMe* pada tahun 2023 dan dampaknya terhadap keamanan individu, dengan fokus pada transformasi data genetik sebagai instrumen kekuasaan dalam kerangka ancaman keamanan non-tradisional. Menggunakan metode deskriptif analitik berbasis kajian literatur, tulisan ini mengeksplorasi tiga dimensi utama, yaitu mekanisme serangan *credential stuffing* yang memanfaatkan fitur *DNA Relatives* sehingga mengekspos jutaan akun pengguna secara global, operasionalisasi biopower korporasi melalui model *Direct-to-Consumer* yang menempatkan *23andMe* sebagai administrator biologis non-negara, serta sifat relasional dan herediter data genetik yang memperluas ancaman kepada jaringan keluarga dan generasi mendatang. Hal tersebut dianalisis melalui integrasi teori biopolitik Michel Foucault dan *human security* dengan dimensi *health security* sebagai kerangka analisis utama. Oleh karena itu, tulisan ini menunjukkan bahwa kebocoran data *23andMe* bukan sekadar kegagalan teknis siber, melainkan manifestas pergeseran logika *bio-surveillance* dari otoritas negara ke ranah korporasi komersial yang menciptakan kerentanan permanen, sistemis, dan tidak merata.

Kata kunci: Biopolitik; Data Genetik; Keamanan Manusia; Keamanan Non-Tradisional; Kebocoran Data.

1. LATAR BELAKANG

Tulisan ini menganalisis fenomena kebocoran data genetik yang terjadi pada perusahaan bioteknologi *23andMe*, yang berdampak pada sekitar 6,9 juta pengguna secara global (Office of The Privacy Commissioner of Canada, 2025). Insiden ini berawal dari serangan siber bertipe *credential stuffing*, di mana pelaku memanfaatkan kredensial pengguna yang bocor dari platform lain untuk mengakses akun secara ilegal (Amishav, 2026). Praktik penggunaan kata sandi yang sama di berbagai layanan digital turut memperbesar kerentanan sistem dan mempermudah eksploitasi terhadap akun pengguna. Fenomena ini menunjukkan bahwa ancaman keamanan siber tidak lagi terbatas pada data digital konvensional, melainkan telah

Naskah Masuk: 12 Mei 2026; Revisi: 23 Mei 2026; Diterima: 25 Juni 2026; Terbit: 29 Juni 2026

merambah ke ranah biologis. Berbeda dengan data seperti kata sandi yang dapat diperbarui, data genetik bersifat permanen, unik, dan melekat pada individu sepanjang hidupnya. Oleh karena itu, kebocoran data genetik tidak hanya menimbulkan pelanggaran privasi, tetapi juga menciptakan kerentanan jangka panjang yang berpotensi memicu diskriminasi berbasis genomik, stigmatisasi sosial, hingga eksklusi struktural di masa depan.

Dalam konteks operasional, *23andMe* merupakan penyedia layanan pengujian genetik berbasis *Direct-to-Consumer* (DTC) yang mengumpulkan dan mengelola data DNA pelanggan melalui sampel saliva. Layanan ini memungkinkan pengguna memperoleh informasi asal-usul keturunan, kondisi kesehatan, serta koneksi kekerabatan genetik melalui fitur *DNA Relatives.* Namun demikian, fitur tersebut justru menjadi titik eskalasi kebocoran data, karena akses terhadap satu akun memungkinkan pelaku menjangkau jaringan kerabat genetik yang lebih luas secara eksponensial (Amishav, 2026). Skala dan dampak kebocoran ini semakin signifikan ketika diketahui bahwa data yang berhasil diperoleh kemudian diperjualbelikan dan dikategorikan berdasarkan identitas etnis tertentu (Satter, 2023). Selain itu, perusahaan juga telah mengakui adanya insiden keamanan tersebut yang kemudian memicu investigasi lintas negara oleh otoritas perlindungan data termasuk kolaborasi antara regulator Inggris dan Kanada, yaitu *Information Commissioner's Office* (ICO) dan *Office of the Privacy Commissioner of Canada* (OPC) (23andMe, 2023). Sebagai bentuk pertanggungjawaban hukum, perusahaan membayar 30 juta dollar serta menyediakan layanan pemantauan keamanan selama tiga tahun untuk menyelesaikan gugatan yang menuduh *23andMe* gagal melindungi 6,9 juta pelanggan yang datanya terekspos dalam kebocoran tersebut (Stempel, 2024).

Perkembangan terbaru semakin mempertegas urgensi persoalan ini. Pada Maret 2025, *23andMe* mengajukan permohonan perlindungan kebangkrutan, yang secara langsung memunculkan pertanyaan mengenai nasib data genetik lebih dari 15 juta penggunanya (Branch, 2025). Dalam proses kebangkrutan tersebut, pengadilan sempat memutuskan bahwa perusahaan dapat menjual basis data genetik sebagai bagian dari aset bisnis, mendorong sejumlah jaksa agung negara bagian untuk mendesak warga mereka agar segera menghaps data dari platform tersebut (Schaefer, 2025). Situasi ini membuktikan bahwa ancaman terhadap kedaulatan biologis individu tidak hanya muncul dari serangan siber eksternal, tetapi juga dari ketidakstabilan institusionaal perusahaan itu sendiri. *Public Citizen* menyoroti bahwa proses kebangkrutan *23andMe* mengekspos celah dalam hukum kepailitan Amerika Serikat, yang belum mampu mengakomodasi perlindungan khusus atas data biologis yang bersifat permanen

dan tidak dapat diperbarui. Hal ini menegaskan bahwa kebocoran data genetik telah berkembang menjadi isu keamanan internasional.

Dalam literatur terdahulu, Callysta Emily Asterina dan Imam Fadhil Nugraha melalui artikelnya *"Reframing Bioterrorism After The 2001 Anthrax Attack: Strategic Shifts In U.S. Counterterrorism Policy"* menjelaskan bahwa ancaman biologis tidak dapat lagi dipahami semata-mata sebagai persoalan kesehatan publik, melainkan telah berubah menjadi instrumen kekuasaan negara yang menyasar kehidupan dan tubuh populasi. Menggunakan keragka biopolitik Michel Foucault, penelitian ini menganalisis bagaimana serangan Anthrax 2001 mendorong Amerika Serikat untuk mengubah orientasi kontraterorisme dari yang bersifat reaktif menjadi preemptif, sekaligus memperluas mekanisme pengawasan biologis atas warganya. Dalam kerangka ini, negara tidak lagi berperan sekadar sebagai pelindung wilayah, melainkan sebagai administrator biologis yang mengatur kondisi kehidupan individu dan sebagai administrator biologis yang mengatur kondisi kehidupan individu dan populasi secara menyeluruh. Penelitian ini juga menyoroti bagaimana pasca serangan Anthrax, sistem *bio-surveillance* yang awalnya dikembangkan untuk tujuan perlindungan kesehatan publik secara bertahap bertransformasi menjadi instrumen kontrol perilaku dan klasifikasi populasi, yang batasnya dengan koersi negara semakn kabur. Temuan ini relevan dengan konteks. Kebocoran data genetik *23andMe*, karena keduanya menunjukkan bagaimana informasi biologis, baik dalam bentuk patogen maupun data DNA, dapat diposisikan sebagai objek strategis kekuasaan yang melampaui dimensi medis semata.

Selanjutnya, Henri-Corto Stoeklé, Marie-France Mamzer-Bruneel, Guillaume Vogt dan Christian Hervé dalam *"23andMe: A New Two-Sided Data-Banking Market Model"* menguraikan bahwa perusahaan ini beroperasi melalui model pasar dua sisi (*two sided market),* yang menghubungkan konsumen individu dengan industri farmasi dan lembaga riset. Dalam model ini, nilai ekonomi utama tidak terletak pada penjualan kit tes DNA, melainkan pada akumulasi data genetik dalam jumlah besar yang kemudian digunakan untuk mendukung penelitian dan pengembangan obat (Henri-Corto Stoeklé, 2016). Dengan demikian, *23andMe* berfungsi sebagai perantara dalam ekosistem data global, di mana pengguna secara tidak langsung menjadi kontributor utama bagi industri bioteknologi. Studi ini juga menekankan bahwa perkembangan model bisnis tersebut berlangsung lebih cepat dibandingkan dengan kesiapan kerangka regulasi, sehingga menciptakan celah kerentanan dalam perlindungan data pengguna.

Melalui tulisannya, Rachele M Hendricks-Sturrup dan Christine Y Lu melalui artikel *"Direct-to-Consumer Genetic Testing Data Privacy: Key Concerns and Recommendations Based on Consumer Persperctives"* menyoroti dimensi kerentanan individu dalam ekosistem DTC *genetic testing*. Penelitian ini menunjukkan bahwa perusahaan *23andMe* memiliki kapasitas untuk membagikan data genetik kepada pihak ketiga, seperti industri farmasi yang sering kali melampaui pemahaman dan ekspektasi pengguna. Selain itu, kompleksitas kebijakan privasi yang digunakan perusahaan menciptakan ketimpangan informasi, di mana konsumen secara formal memberikan persetujuan tanpa benar-benar memahami implikasinya (Rachele M Hendricks-Sturrup, 2019). Penelitian ini juga menemukan bahwa risiko tidak bersifat merata, melainkan dipengaruhi oleh posisi sosial individu. Kelompok minoritas dan kelompok rentan cenderung menghadapi risiko yang lebih besar, termasuk potensi diskriminasi berbasis data genetik. Studi ini juga menggarisbawahi keterbatasan regulasi yang ada, yang belum mampu memberikan perlindungan menyeluruh terhadap penggunaan dan penyalahgunaan data biologis.

Meskipun ketiga literatur tersebut memberikan kontribusi penting, masing-masing masih memiliki keterbatasan. Callysta dan Imam Fadhil mengkaji biopolitik dalam konteks kebijakan negara, namun tidak menyentuh bagaimana logika *bio-surveillance* kini bermigrasi ke ranah korporasi swasta. Stoeklé et al. menjelaskan model bisnis data genetik, tetapi belum mengkaji implikasi keamanan ketika data tersebut bocor. Sementara Hendricks-Sturrup dan Lu masih terbatas pada dimensi privasi dan regulasi, belum menjangkau kebocoran data genetik sebagai ancaman keamanan non-tradisional yang berdampak lintas generasi.

Oleh karena itu, penelitian ini mengisi kekosongan tersebut dengan menganalisis kebocoran data *23andMe* melalui pendekatan *human security* dan biopolitik Michel Foucault, untuk memahami bagaimana data genetik tidak hanya menjadi komoditas ekonomi, tetapi juga instrumen kekuasaan yang mengancam keamanan individu secara permanen. Dengan demikian, penelitian ini menempatkan kebocoran data genetik sebagai transformasi ancaman dalam hubungan internasional yang memperluas makna keamanan dari sekadar ancaman digital menuju ancaman biologis.

2. KAJIAN TEORITIS

Penelitian mengenai kebocoran data genetik pada *23andMe* ini dianalisis menggunakan dua teori utama, yaitu *human security* dengan fokus pada *health security*, serta teori biopolitik dari Michel Foucault. Kedua teori ini digunakan untuk menjelaskan pergeseran ancaman

keamanan dari yang berorientasi pada negara menuju individu, khususnya dalam konteks perkembangan bioteknologi dan digital.

Teori *human security* yang diperkenalkan oleh *United Nations Development Programme* dalam *Human Development Report* 1994 menempatkan individu sebagai pusat dari konsep keamanan. Salah satu dimensinya adalah *health security*, yang menekankan perlindungan terhadap ancaman yang membahayakan kondisi biologis manusia (United Nations Development Programme, 1994). Dalam perkembangan kontemporer, ancaman terhadap *health security* tidak hanya berasal dari penyakit, tetapi juga dari penyalahgunaan informasi biologis. Oleh karena itu, kebocoran data genetik dapat dipahami sebagai ancaman terhadap *health security* karena berpotensi menimbulkan diskriminasi, eksploitasi, serta kerentanan jangka panjang atau bahkan selamanya bagi individu. Perkembangan terbaru menunjukkan bahwa cakupan *health security* kini tidak lagi terbatas pada ancaman penyakit konvensional. Kemajuan teknologi digital dan biologis telah melahirkan ancaman baru yang dikenal sebagai *cyberbiosecurity*, yaitu kondisi ketika data biologis seperti informasi genomik menjadi sasaran serangan siber. Ancaman ini tidak hanya berdampak pada sektor kesehatan, tetapi juga dapat memengaruhi keamanan individu dan masyarakat (Fouad, 2024).

Sementara itu, teori biopolitik dari Michel Foucault menjelaskan bahwa kekuasaan modern beroperasi melalui pengelolaan kehidupan *(biopower)*, yaitu kontrol terhadap tubuh dan populasi melalui produksi serta pengelolaan pengetahuan biologis (Foucault, 2008). Dalam kerangka ini, data genetik menjadi objek strategis yang dapat dikontrol dan dimanfaatkan oleh aktor tertentu. Penguasaan data genetik oleh entitas seperti *23andMe* mencerminkan bentuk kekuasaan baru yang bersifat asimetris, di mana individu kehilangan kontrol atas identitas biologisnya. Kebocoran data genetik semakin memperlihatkan bagaimana informasi biologis dapat digunakan sebagai instrumen klasifikasi dan kontrol terhadap individu di luar kendalinya (Foucault, 2008). Dengan demikian, kedua teori ini menunjukkan bahwa kebocoran data genetik tidak hanya menerapkan isu keamanan siber, tetapi juga merupakan bentuk ancaman dalam keamanan non-tradisional yang menyasar dimensi biologis individu secara langsung.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif analitik yang berfokus pada kajian literatur *(literature review)*. Metode ini bertujuan untuk mengkaji fenomena kebocoran data genetik secara sistematis dengan memberikan gambaran yang komprehensif mengenai implikasinya terhadap keamanan individu, khususnya dalam kerangka teori *human security* dan biopolitik. Dengan pendekatan ini, penelitian tidak hanya

mendeskripsikan fenomena, tetapi juga menganalisis makna dan implikasi yang muncul dari kebocoran data genetik dalam konteks keamanan non-tradisional.

Pengumpulan data dilakukan melalui studi pustaka yang mencakup artikel jurnal ilmiah, laporan hasil investigasi lembaga resmi, publikasi organisasi terkait, sumber media internasional yang kredibel, serta didukung oleh literatur buku yang relevan. Data yang diperoleh kemudian dianalisis secara deskriptif untuk mengidentifikasi pola, hubungan, serta implikasi dari kasus kebocoran data pada *23andMe*, sehingga menghasilkan pemahaman yang komprehensif mengenai bagaimana data genetik bertransformasi menjadi sumber kerentanan sekaligus instrumen kekuasaan dalam dinamika keamanan global.

4. HASIL DAN PEMBAHASAN

Dalam menganalisis implikasi kebocoran data genetik 23andMe terhadap keamanan individu, penting untuk terlebih dahulu memahami bagaimana insiden ini terjadi secara teknis dan mengapa dampaknya jauh melampaui kebocoran data digital pada umumnya. Berbeda dengan data konvensional yang dapat diperbarui, data genetik bersifat permanen dan mengandung informasi tidak hanya tentang satu individu, tetapi juga seluruh jaringan keluarga biologisnya. Hal inilah yang menjadikan kebocoran data 23andMe sebagai ancaman yang unik dan mendesak untuk dikaji lebih dalam melalui pendekatan keamanan non-tradisional. Tulisan ini mengkaji bagaimana kebocoran data tersebut mencerminkan pergeseran logika kekuasaan atas informasi biologis dari ranah negara menuju korporasi swasta, serta bagaimana pergeseran tersebut berdampak langsung pada keamanan dan kesejahteraan individu. Melalui integrasi kerangka biopolitik Michel Foucault dan human security, analisis ini memperlihatkan bahwa 23andMe tidak sekadar gagal melindungi data penggunanya, tetapi juga mencerminkan absennya akuntabilitas korporasi dalam mengelola informasi biologis yang nilainya terus meningkat seiring perkembangan teknologi.

Oleh karena itu, melalui pembahasan ini akan diuraikan lebih lanjut mengenai bagaimana mekanisme serangan credential stuffing mengeksploitasi desain fitur DNA Relatives sehingga menghasilkan kebocoran yang bersifat berantai dan masif, bagaimana data genetik bertransformasi menjadi instrumen kekuasaan dan komoditas ilegal yang dikategorikan berdasarkan etnisitas, serta bagaimana keterbatasan regulasi yang ada membiarkan individu, terutama kelompok rentan, menanggung ancaman diskriminasi genomik yang bersifat permanen dan bahkan dapat diwariskan kepada generasi mendatang.

Kronologi dan Mekanisme Kebocoran Data 23andMe

Untuk memahami dampak yang ditimbulkan, bagian ini menjelaskan bagaimana kebocoran data *23andMe* terjadi secara berurutan. Penting untuk dipahami bahwa insiden ini tidak terjadi karena peretasan langsung terhadap sistem utama perusahaan, melainkan melalui serangkaian proses yang dimulai dari luar dan berakhir pada ancaman yang nyata bagi keamanan individu. Titik awal kebocoran data berasal dari beredarnya kombinasi nama pengguna dan kata sandi yang sebelumnya telah bocor dari platform digital lain. Data ini kemudian dimanfaatkan oleh pelaku untuk melancarkan serangan *credential stuffing,* yaitu percobaan otomatis ribuan kombinasi akun bocor tersebut ke dalam sistem *login 23andMe* (Amishav, 2026). Serangan ini berhasil karena banyak pengguna menggunakan kata sandi yang sama di berbagai platform, sehingga ketika satu platform bocor, akun mereka di platform lain ikut terancam. Analisis terhadap insiden ini menunjukkan bahwa serangan bermulai ketika seorang pelaku dengan nama samaran "Golem" mengklaim telah membobol data lebih dari 4 juta pengguna dan mempublikasikan sebagian data. Tersebut di forum peretasan *BreachForums* sebagai bukti. Pada tahap awal, sekitar 14.000 akun berhasil dikompromikan secara langsung melalui serangan *credential stuffing.* Namun, dampaknya berkembang jauh lebih besar karena fitur DNA Realtives memungkinkan akun yang telah diretas mengakses jaringan profil genetik lain yang saling terhubung. Akibatnya, pelanggaran tersebut meluas hingga mengekspos data pribadi dan genetik sekitar 5,5 juta pengguna tambahan, serta sekitar 1,4 juta profil lain dari fitur *family tree* (Holthouse, Owens, & Bhunia, 2025).

Fakta ini menunjukkan bahwa titik kerentanan utama bukan hanya terletak pada lemahnya kata sandi pengguna, tetapi juga pada desain fitur berbagi data yang memungkinkan satu titik menghasilkan dampak yang berlipat ganda. Data yang berhasil dikumpulkan kemudian diperjualbelikan di forum-forum peretasan termasuk *dark web* dan dikategorikan berdasarkan identitas etnis tertentu (Satter, 2023). Pada titik inilah kebocoran ini berubah dari insiden teknis menjadi ancaman serius bagi keamanan individu, karena informasi biologis yang bersifat permanen kini berada di tangan pihak yang tidak bertanggung jawab.

Data Genetik sebagai Instrumen Kekuasaan dan Ancaman Individu

Mekanisme kebocoran yang telah diuraikan tidak dapat dianalisis hanya dari sudut pandang keamanan konvensional. Untuk memahami implikasinya secara menyeluruh, diperlukan dua kerangka teori yang bekerja secara terintegrasi, yaitu biopolitik Foucault dan *human security*. Biopolitik menjelaskan bagaimana penguasaan data genetik mencerminkan

relasi kekuasaan yang simetris, sementara *human security* memperlihatkan bagaimana relasi kekuasaan tersebut berdampak langsung pada keamanan dan kesejahteraan individu.

Dalam kerangka biopolitik, *23andMe* tidak hanya beroperasi sebagai perusahaan teknologi kesehatan biasa. Dengan mengakumulasi data DNA jutaan pengguna melalui model *Direct-to-Consumer,* perusahaan ini menjalankan logika biopower dalam bentuk baru, yaitu sebagai aktor korporasi non-negara yang mengelola dan mengontrol informasi biologis populasi dalam skala masif (Rachele M Hendricks-Sturrup, 2019). Callysta dan Imam Fadhil (2024) menjelaskan bahwa dalam kerangka biopolitik, negara berkembang menjadi "administrator biologis yang mengatur kondisi kehidupan individu dan populasi secara menyeluruh". Dalam kasus *23andMe,* peran tersebut diambil alih oleh korporasi swasta yang beroperasi tanpa akuntabilitas publik yang setara. Dari perspektif *human security,* kondisi ini menempatkan individu dalam posisi yang rentan sejak awal, karena mereka tidak memiliki kendali nyata atas informasi biologis yang telah mereka serahkan kepada perusahaan.

Ketika kebocoran terjadi, relasi kekuasaan yang asimetris ini semakin memperparah kerentanan individu. Biopower yang semula dipegang oleh korporasi berpindah ke tangan aktor yang tidak bertanggung jawab dan data genetik yang dikategorikan berdasarkan identitas etnis menjadi instrumen potensial untuk klasifikasi dan diskriminasi populasi. Sistem *bio-surveillance* yang awalnya dikembangkan untuk tujuan perlindungan kesehatan publik secara bertahap berubah menjadi instrumen kontrol perilaku dan klasifikasi populasi (Callysta Emily Asterina, 2024). Transformasi yang sama terjadi dalam kasus *23andMe*, bukan melalui kebijakan negara, melainkan melalui platform bioteknologi komersial yang mengakumulasi kemudian kehilangan kendali atas data biologis jutaan penggunanya. Dalam perspektif *human security*, hal ini secara konkret mengancam ranah *health security* individu karena data tantang predisposisi penyakit dan latar belakang biologis kini dapat diakses dan disalahgunakan oleh pihak mana pun.

Ancaman ini men.jadi lebih kompleks karena sifat relasional dari data genetik. Berbeda dari jenis data lain yang hanya menyangkut satu individu, data genetik secara inheren mengandung informasi tentang seluruh jaringan keluarga biologis pemiliknya (Bonomi, Huang, & Ohno-Machado, 2020). Melalui fitur *DNA Relatives,* satu akun yang dikompromi dapat mengekspos data ribuan individu lain yang tidak pernah memberikan persetujuan apapun. Sebagaimana diidentifikasi oleh Hendricks-Sturrup dan Lu (2019), kelompok minoritas dan kelompok yang lebih rentan secara sosial menghadapi risiko yang jauh lebih besar, sejalan dengan temuan Callysta dan Imam Fadhil (2024) yang

menunjukkan bahwa ancaman biologis "dapat memicu stigmatisasi sosial hingga pengucilan atau ketidakadilan dalam akses pekerjaan, asuransi, dan layanan sosial" bagi kelompok-kelompok tertentu. Dalam kerangka *human security*, ketidakmerataan ini menegaskan bahwa kebocoran data genetik bukan ancaman yang netral, melainkan ancaman yang secara struktural lebih berat ditanggung oleh mereka yang sudah lebih dulu berada dalam posisi rentan.

Ancaman ini juga tidak bersifat sementara karena data genetik bersifat permanen dan nilainya berpotensi meningkat seiring perkembangan teknologi analisis biologis, data yang bocor hari ini dapat disalahgunakan di masa depan dengan cara yang belum sepenuhnya dapat diprediksi. Seseorang dapat menghadapi diskriminasi dalam akses pekerjaan, asuransi kesehatan, atau layanan publik berdasarkan informasi genetik yang tersebar tanpa sepengetahuannya. Karena data genetik juga mencerminkan informasi tentang keturunan, ancaman ini berpotensi diwariskan kepada generasi berikutnya yang sama sekali tidak terlibat dalam keputusan awal penggunaan layanan. Meskipun regulasi seperti *Genetic Information Nondiscrimination Act* (GINA) di Amerika Serikat telah berupaya memberikan perlindungan, jangkauannya masih sangat terbatas dalam konteks global ketika data telah beredar di luar kendali hukum formal.

Dalam konteks Amerika Serikat, GINA yang disahkan pada 2008 memang melarang diskriminasi berbasis informasi genetik dalam ranah asuransi kesehatan dan ketenagakerjaan, namun seorang penulis mengingatkan bahwa undang-undang ini lahir sebagai regulasi preemptif, yaitu respons terhadap ancaman yang dikhawatirkan terjadii, bukan terhadap diskriminasi yang sudah terdokumentasi secara luas (Suter, 2018). GINA juga memiliki celah struktural yang signifikan, seperti undang-undang ini tidak mencakup asuransi jiwa, asuransi disabilitas, dan asuransi perawatan jangka panjang, serta tidak berlaku bagi perusahaan dengan kurang dari 15 karyawan. Seiring meningkatnya akurasi dan kekuatan prediktif pengujian genetik, celah-celah ini berpotensi diekploitasi, terutama terhadap kelompok yang sudah rentan secara sosial (Chapman, Mehta, Parent, & Caplan, 2020). Dalam konteks kebocoran data *23andMe*, ini berarti bahwa individu yang datanya telah tersebar luas di *dark web* tidak memiliki mekanisme hukum yang efektif untuk mencegah kemungkinan diskriminasi di masa depan, khususnya dalam ranah yang tidak dicakup oleh GINA.

Maka dari itu, analisis menggunakan biopolitik dan *human security* ini memperlihatkan bahwa kebocoran data *23andMe* merupakan manifestasi dari perubahan ancaman keamanan non-tradisional di era bioteknologi. Biopolitik menjelaskan bagaimana

struktur kekuasaan yang asimetris antara korporasi dan individu memungkinkan terjadinya eksploitasi data biologis dalam skala masif. *Human security* menjelaskan siapa yang paling terdampak dan mengapa perlindungan terhadap individu harus menjadi pusat dari respons kebijakan yang dibangun. Keduanya sama-sama menegaskan bahwa perlindungan data biologis harus dipahami tidak hanya sebagai persoalan privasi digital, melainkan sebagai bagian integral dari agenda keamanan individu dan keamanan internasional yang mendesak untuk segera ditangani.

Implikasi dari seluruh rangkaian ancaman ini telah melampaui ranah privasi individu dan memasuki agenda keamanan internasional secara formal. Ketika proses kebangkrutan *23andMe* berlangsung pada 2025, anggota kongres Amerika Serikat James Comer secara eksplisit menyatakan bahwa kepemilikan masa depan atas basis data genetik 23andMe bukan hanya persoalan bisnis atau rstrukturisasi, melainkan *"a matter of national security"* (Kimery, 2025). Pernyataan ini mencerminkan pengakuan bahwa data genomik dalam skala masif dapat menjadi instrumen strategis yang melampaui kepentingan korporasi, baik sebagai alat intelijen, basis diskriminasi populasi, maupun komoditas geopolitik yang bernilai tinggi. Keamanan data genomik terus menghadapi ancaman baru seiring perkembangan teknologi analisis biologis, bahkan ketika data tersebut disimpan dalam lingkungan komputasi yang dianggap aman. Dengan demikian, kebocoran data *23andMe* tidak hanya mencerminkan. Kegagalan teknis atau korporasi, tetapi juga menjadi peringatan bagi komunitas internasional bahwa tata kelola data biologis harus menjadi agenda bersama dalam pembangunan keamanan global (Kuo, et al., 2022)

5. KESIMPULAN DAN SARAN

Penelitian ini menjawab permasalahan mengenai implikasi kebocoran data genetik *23andMe* dengan membuktikan bahwa insiden tersebut bukan sekadar kegagalan teknis siber, melainkan sebuah transformasi ancaman keamanan non-tradisional yang menyasar kedaulatan biologis individu. Melalui pisau analisis biopolitik Michel Foucault, ditemukan fakta bahwa logika *bio-surveillance* kini telah berpindah dari otoritas negara ke ranah korporasi komersial. *23andMe* bertindak sebagai administrator biologis baru yang mengumpulkan data DNA dalam model *two-sided market,* namun gagal memitigasi risiko asimetris kekuasaan saat data tersebut bocor dan dikomodifikasi secara ilegal berdasarkan etnisitas di *dark web.* Sementara itu, pendekatan *human security* mengonfirmasi bahwa dampak kebocoran ini menciptakan kerentanan permanen, sistemis, dan herediter. Sifat relasional data genetik menyebabkan ancaman diskriminasi genomik dan stigmatisasi sosial tidak hanya menimpa pengguna

langsung, melainkan meluas kepada jaringan keluarga serta generasi masa depan yang tidak pernah memberikan konsen.

Berdasarkan hal tersebut, direkomendasikan adanya rekonstruksi regulasi tata kelola data biologis global yang tidak lagi menyamakan data genetik dengan data digital konvensional. Proses kebangkrutan *23andMe* pada 2025 mengungkap celah lainnya, seperti hukum kepailitan yang berlaku saat ini belum dirancang untuk mengakomodasi perlindungan khusus atas data biologis yang bersifat permanen. Ketika perusahaan bangkrut, data genetik jutaan pengguna berpotensi diperlakukan setara dengan aset properti biasa yang dapat dialihkan kepada pemilik baru tanpa persetujuan ulang (Branch, 2025). Oleh karena itu, diperlukan pembaruan mendesak pada kerangka hukum kepailitan di berbagai yurisdiksi untuk secara eksplisit mengakui data biologis sebagai kategori aset khusus yang tidak dapat diperjualbelikan tanpa mekanismee perlindungan dan persetujuan pengguna yang ketat.

Otoritas perlindungan data internasional perlu menyusun standar hukum yang mengikat bagi perusahaan *Direct-to-Consumer genetic testing*, termasuk kewajiban transparansi penuh, audit keamanan siber berlapis, dan pelarangan tegas terhadap kategorisasi data berdasarkan ras atau etnis. Bagi masyarakat, diperlukan peningkatan literasi digital pada bidang biologis yang kritis sebelum menyerahkan sampel DNA ke platform komersial. Di sisi lain, penelitian ini memiliki keterbatasan karena sifatnya yang berbasis kajian literatur deskriptif analitik, sehingga generalisasi dampak jangka panjang masih bersifat teoretis dan bergantung pada dinamika perkembangan teknologi di masa depan. Oleh karena itu, penelitian yang akan datang disarankan untuk menggunakan metode empiris, seperti studi pelacakan korban terdampak secara hukum atau analisis komparatif mengenai efektivitas regulasi perlindungan data genomik di berbagai yurisdiksi negara yang berbeda.

DAFTAR REFERENSI

Office of The Privacy Commissioner of Canada. (2025). *Backgrounder: Summary of joint investigation into data breach at 23andMe by the Privacy Commissioner of Canada and the UK Information Commissioner.* Office of The Privacy Commissioner of Canada.

Amishav, J. (2026, January 18). *Blog: 23andMe Data Breach: How Credential Stuffing Exposed 7 Million Genetic Profiles*. Diambil kembali dari 23andMe Data Breach: How Credential Stuffing Exposed 7 Million Genetic Profiles: https://www.breachsense.com/blog/23andme-data-breach-case-study/

Amishav, J. (2026, January 18). *Blog: 23andMe Data Breach: How Credential Stuffing Exposed 7 Million Genetic Profiles*. Diambil kembali dari 23andMe Data Breach: How Credential Stuffing Exposed 7 Million Genetic Profiles: https://www.breachsense.com/blog/23andme-data-breach-case-study/

Satter, R. (2023, october 6). *Technology: Hackers advertise sale of 23andMe data on leaked data forum* . Diambil kembali dari Hackers advertise sale of 23andMe data on leaked data forum : https://www.reuters.com/technology/hackers-advertise-sale-23andme-data-leaked-data-forum-2023-10-06/

23andMe. (2023, october 6). *Blog: Addressing Data Security Concerns – Action Plan.* Diambil kembali dari Addressing Data Security Concerns – Action Plan: https://blog.23andme.com/articles/addressing-data-security-concerns

Stempel, J. (2024, september 13). *Technology: cybersecurity:* . Diambil kembali dari 23andMe settles data breach lawsuit for $30 million: https://www.reuters.com/technology/cybersecurity/23andme-settles-data-breach-lawsuit-30-million-2024-09-13/

Branch, J. (2025, July 15). *article: House Must Update Bankruptcy Code in Wake of 23andMe DNA Data Sale*. Diambil kembali dari House Must Update Bankruptcy Code in Wake of 23andMe DNA Data Sale: https://www.citizen.org/article/house-must-update-bankruptcy-code-in-wake-of-23andme-dna-data-sale/

Schaefer, E. (2025, July 9). *news: 23andMe's 2023 Data Breach and Contradictions in Current Regulatory Frameworks* . Diambil kembali dari 23andMe's 2023 Data Breach and Contradictions in Current Regulatory Frameworks : https://jsis.washington.edu/news/23andmes-2023-data-breach-and-contradictions-in-current-regulatory-frameworks/

Henri-Corto Stoeklé, M.-F. M.-B. (2016). 23andMe: a new two-sided data-banking market model. *BMC Medical Ethics*, 1-11.

Rachele M Hendricks-Sturrup, C. Y. (2019). Direct-to-Consumer Genetic Testing Data Privacy: Key Concerns and Recommendations Based on Consumer Perspectives. *Journal of Personalized Medicine*, 1-5.

United Nations Development Programme. (1994, july 7). *publications: human development report.* Diambil kembali dari human development report: https://hdr.undp.org/system/files/documents/hdr1994encompletenostats.pdf

Fouad, N. S. (2024, april 29). *core: journals: Cyberbiosecurity in the new normal: Cyberbio risks, pre-emptive security, and the global governance of bioinformation.* Diambil kembali dari Cyberbiosecurity in the new normal: Cyberbio risks, pre-emptive security, and the global governance of bioinformation: https://doi.org/10.1017/eis.2024.19

Foucault, M. (2008, september). *The Birth of Biopolitics: Lectures at the Collège de France, 1978- 1979.* New York: Palgrave Macmillan. Diambil kembali dari Michel Foucault, The Birth of Biopolitics: Lectures at the Collège de France, 1978- 1979. Edited by Michel Senellart. Translated by Graham Burchell: https://scispace.com/pdf/michel-foucault-the-birth-of-biopolitics-lectures-at-the-48zqfn9gm5.pdf

Holthouse, R., Owens, S., & Bhunia, S. (2025). The 23andMe Data Breach: Analyzing Credential Stuffing Attacks, Security Vulnerabilities, and Mitigation Strategies. *arXiv*, 1-6.

Callysta Emily Asterina, I. F. (2024). Reframing Bioterrorism After The 2001 Anthrax Attack: Strategic Shifts In U.S. Counterterrorism Policy. *Indonesian Journal of Counter Terrorism and National Security*, 322-348.

Bonomi, L., Huang, Y., & Ohno-Machado, L. (2020). Privacy challenges and research opportunities for genomic data sharing. *Nature Genetics*, 646-654.

Chapman, C. R., Mehta, K. S., Parent, B., & Caplan, A. L. (2020). Genetic Discrimination: Emerging Ethical Challenges in the Context of Advancing Technology. *Journal of Law and the Biosciences*, 2-22.

Kimery, A. (2025, june 11). *biometric news: US lawmakers sound alarm over genetic data vulnerabilities in 23andMe bankruptcy case*. Diambil kembali dari US lawmakers sound alarm over genetic data vulnerabilities in 23andMe bankruptcy case: https://www.biometricupdate.com/202506/us-lawmakers-sound-alarm-over-genetic-data-vulnerabilities-in-23andme-bankruptcy-case

Kuo, T.-T., Jiang, X., Tang, H., Wang, X., Harmanci, A., Kim, M., . . . Ohno-Machado, L. (2022). The Evolving Privacy and Security Concerns for Genomic Data Analysis and Sharing as Observed from the iDASH Competition. *Journal of the American Medical Informatics Association (JAMIA)*, 2182-2188.