Amanna Gappa

**Amanna Gappa, Vol. 28 No. 2, 2020**
*Terakreditasi Nasional SINTA 4*

P-ISSN: 0853-1609, E-ISSN: 2549-9785
***Fakultas Hukum Universitas Hasanuddin***

# Praktik Penyalahgunaan Fitur Kredit (*Paylater*) oleh Pihak Ketiga melalui Aplikasi Belanja Online

**Andi Pratiwi Yasni Putri*, Ahmadi Miru, Maskun**

*Fakultas Hukum Universitas Hasanuddin, Indonesia.*
* *E-mail: andipratiwiyasniputri@gmail.com*

***Abstract:***

*This study aims to determine the legal protection of users of online shopping services based on applications for misuse of paylater features by third parties. This research is a normative-empirical research. The research was conducted in Makassar City, namely the Regional Financial Services Authority 6 and in several online shopping application companies that provide paylater services, such as PT. Trinusa Travelindo (Traveloka), PT. Karya Anak Bangsa (Gojek) application, and PT. Shopee International Indonesia (Shopee). The results show that legal protection against consumers for abuse of credit features (paylater) by third parties through online shopping applications has been implemented by paylater feature service providers, where legal protection is oriented towards preventive (preventive) measures, such as working together with a certified institution in storing and maintaining the security of service user data/information, implementing a layered security system, and providing education to service users. With regard to cases of break-in paylater accounts that have occurred, generally the service provider is not responsible as stated in the privacy policy for service use, so that the burden of losses arising from cases of account breach is still borne by consumers.*

***Keywords:*** *e-Commerce; Cyberspace; Credit card; Paylater; Fraud*

***Abstrak:***

*Penelitian ini bertujuan untuk mengetahui perlindungan hukum terhadap pengguna layanan belanja online berbasis aplikasi atas penyalahgunaan fitur paylater oleh pihak ketiga. Penelitian ini adalah penelitian normatif-empiris. Penelitian dilakukan di Kota Makassar, yaitu Otoritas Jasa Keuangan Regional 6 dan pada beberapa perusahaan aplikasi belanja online yang menyediakan layanan paylater, seperti PT. Trinusa Travelindo (Traveloka), PT. Aplikasi Karya Anak Bangsa (Gojek), dan PT. Shopee International Indonesia (Shopee). Hasil penelitian menunjukkan bahwa perlindungan hukum terhadap konsumen atas penyalahgunaan fitur kredit (paylater) oleh pihak ketiga melalui aplikasi belanja online telah diterapkan oleh para penyedia jasa fitur paylater. Perlindungan hukum berorientasi pada upaya-upaya yang bersifat preventif (pencegahan), seperti bekerja sama dengan lembaga tersertifikasi di dalam menyimpan dan menjaga keamanan data-data/informasi pengguna, menerapkan sistem keamanan berlapis, dan memberikan edukasi kepada para pengguna jasa. Terhadap kasus pembobolan akun paylater yang telah terjadi, pada umumnya penyedia jasa tidak bertanggung jawab sebagaimana telah ditegaskan di dalam kebijakan privasi penggunaan layanan, sehingga beban kerugian yang timbul akibat kasus pembobolan akun tetap dipikul oleh konsumen.*

***Kata Kunci:*** *e-Commerce; Cyberspace; Kartu Kredit; Paylater; Penipuan*

## 1. Pendahuluan

Dampak globalisasi telah membawa perubahan signifikan di seluruh sektor kehidupan manusia, termasuk perkembangan pesat teknologi dan internet. Teknologi dan internet memiliki peran yang begitu besar dalam menunjang segala aktivitas kehidupan manusia sehingga berdampak bagi beberapa sektor, seperti pada sektor bisnis atau industri bisnis yang kemudian perkembangan dalam industri perdagangan dan industri keuangan di Indonesia.[1] Transaksi perdagangan yang kini telah berkembang pesat sebagai dampak perpaduan teknologi internet melahirkan suatu sistem perdagangan *online* yang disebut *e-commerce*. Lahirnya *e-commerce* memberikan dampak positif karena kemudahan transaksi yang diciptakan, seperti penghematan waktu, kebebasan konsumen untuk memilih barang dan/atau jasa yang dibutuhkan dengan harga yang sangat kompetitif.[2]

*E-commerce* merupakan suatu bentuk pemanfaatan teknologi informasi dan transaksi elektronik sebagaimana diatur dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Salah satu tujuannya adalah untuk mengembangkan perdagangan dan perekonomian nasional dalam rangka meningkatkan kesejahteraan rakyat.[3] *E-commerce* menghadirkan model bisnis modern yang *non-face* (tidak menghadirkan pelaku bisnis secara fisik) dan *non-sign* (tidak memakai tanda tangan asli). Tentu saja dengan model bisnis ini di katakan lebih praktis dan lebih mudah. Praktis Kondisi itu menyebabkan jarak bukan lagi menjadi hambatan dalam dunia bisnis, sehingga para pelaku usaha dapat melakukan transaksi tanpa harus bertemu secara langsung.[4]

Praktik berbelanja *online* dilakukan antara penjual dan pembeli yang tidak bertemu secara langung dengan pembayaran dilakukan melalui via transfer antarbank ataupun menggunakan kartu kredit. Setelah pemesanan dilakukan, konsumen melakukan pembayaran *online* dengan mengisi data kartu kredit (nama pemegang kartu, nomor kartu kredit, masa berlaku kartu kredit, 3 angka kode CVC/CVV, dan alamat penagihan). Namun, saat ini, di samping metode pembayaran via transfer dan kartu kredit yang disediakan, beberapa pelaku usaha belanja *online* juga telah menghadirkan fitur pembayaran tanpa kartu kredit, yang dikenal dengan fitur bayar kemudian atau *Paylater*.

Sesuai dengan namanya, fitur *PayLater* memberikan konsumen kesempatan untuk memanfaatkan jasa dan layanan sementara mereka membayar diakhir sesuai dengan batas waktu yang diberikan. Kemunculan fitur *paylater* adalah hasil kerja sama antara perusahaan belanja *online* dengan perusahaan pembiayaan berbasis *peer to peer lending*. *Peer to peer lending* merupakan suatu layanan pinjam meminjam berbasis teknologi informasi yang mempertemukan pemberi pinjaman dengan para pencari pinjaman

---

[1] Budiharto Ernama & Hendro. (2017). Pengawasan Otoritas Jasa Keuangan Terhadap Financial Technology (Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016). *Diponegoro Law Journal*, Vol. 6, No. 3: 1-12.

[2] Ning Rahayu, *Ini Dampak Perkembangan E-Commerce Bagi Indonesia*, https://www.wartaekonomi.co.id/read216033/ini-dampak-perkembangan-e-commerce-bagi-indonesia.html diakses tanggal 2 April 2020.

[3] Pasal 4 huruf b Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[4] Imam Sjahputra, 2010. *Perlindungan Konsumen Dalam Transaksi Elektronik*. Alumni, Bandung, hlm. 2.

(*borrower*) di dalam sebuah wadah atau perusahaan.[5] *Peer to peer lending* saat ini diatur dalam Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. Seperti halnya *e-commerce*, *peer to peer lending* adalah suatu wadah pinjam meminjam yang juga dilakukan secara *online*, yang tidak membutuhkan adanya tatap muka secara langsung antara penerima pinjaman[6] dengan pemberi pinjaman.[7]

Terlepas dari kemudahan-kemudahan yang didapatkan dalam *transaksi e-commerce*, faktor keamanan akun konsumen juga merupakan salah satu hal yang tidak kalah penting yang wajib diperhatikan oleh pelaku usaha. Hal ini disebabkan meskipun skema transaksi jual beli dilakukan melalui *e-commerce*, namun sesuai dengan ketentuan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (UUPK), maka hak-hak serta kewajiban konsumen maupun pelaku usaha yang diatur dalam UUPK tidak dapat dikesampingkan dan tetap berlangsung.

Semakin mudahnya akses transaksi elektronik dalam *e-commerce* juga harus seiring dengan semakin ketatnya faktor keamanan data konsumen guna untuk mencegah tindakan penyalahgunaan data atau pembobolan akun oleh pihak ketiga. Namun, berdasarkan fakta yang terjadi, kehadiran fitur pembayaran *PayLater* telah membuka suatu peluang yang baru bagi pihak-pihak yang tidak bertanggungjawab untuk melakukan pembobolan akun. Salah satunya yang terjadi pada konsumen MR pengguna layanan *PayLater* melalui aplikasi Traveloka. Pada tanggal 14 Maret 2019, MR tiba-tiba menemukan ada transaksi sebesar kurang lebih Rp.1.300.000,- (satu juta tiga ratus ribu rupiah) untuk pembelian tiket tujuan Jakarta ke Padang dengan dan pembayaran menggunakan *PayLater*. Karena merasa tidak pernah melakukan pembelian tersebut, MR akhirnya menghubungi *customer service* Traveloka. Alhasil, dari tanggapan pihak Traveloka hanya disebutkan bahwa pelanggan tersebut tetap harus membayar transaksi tersebut karena sudah menjadi kewajiban MR untuk menjaga keamanannya. Hal ini bukan hanya terjadi pada satu konsumen, melainkan sudah pada beberapa konsumen.[8]

Selain pada layanan *paylater* yang tersedia di aplikasi Traveloka, layanan *paylater* yang bekerja sama dengan aplikasi belanja *online* lainnya juga kerap kali menjadi sasaran para *hacker* untuk melakukan pembobolan. Salah satu kasus yang terjadi, yakni seorang pengguna layanan Shopeepay dengan *username* arleen_04 mengalami kasus pembobolan pada akun Shopeepay sebesar Rp. 1.900.000,- (satu juta sembilan ratus ribu rupiah). Akun *paylater* milik arleen_04 digunakan *hacker* melakukan transaksi pembelian perdana kuota dengan menggunakan metode pembayaran Shopeepay *later*, dan secara otomatis pihak korban membatalkan transaksi tersebut karena merasa bukan transaksi yang dilakukannya. Akan tetapi, *hacker* tersebut kembali melanjutkan

---

[5] Sarah Safira Aulianisa. 2020. "Konsep Dan Perbandingan Buy Now, Pay Later Dengan Kredit Perbankan Di Indonesia: Sebuah Keniscayaan Di Era Digital Dan Teknologi." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional,* Vol. 9, no. 2: 183-194.

[6] Pasal 1 angka 7 POJK No. 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi : "Penerima Pinjaman adalah orang dan/atau badan hukum yang mempunyai utang karena perjanjian Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi."

[7] Pasal 1 angka 8 POJK No. 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi : "Pemberi Pinjaman adalah orang, badan hukum, dan/atau badan usaha yang mempunyai piutang karena perjanjian Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi."

[8] Meylinda Rachmadanniar. *Paylater Traveloka Dipakai Orang Lain Dan Lagi-Lagi Pelanggan Disalahkan.* https://mediakonsumen.com/2019/03/14/surat-pembaca/paylater-traveloka-dipakai-orang-lain-dan-lagi-lagi-pelanggan-disalahkan diakses tanggal 16 September 2019.

transaksi tersebut dan korbanpun tidak bisa membatalkan transaksi tersebut karena ada notifikasi dari Shopee bahwa korban tidak dapat membatalkan transaksi karena sudah sekali melakukan pembatalan. Namun, setelah menyampaikan keluhan dan keberatan tersebut kepada pihak Shopee, akun yang dibobol tersebut telah kembali dipulihkan dan setelah 3 (tiga) hari korban melihat transaksi tersebut masih dilanjutkan oleh pihak Shopee dan berstatus dalam pengiriman.[9]

Kasus yang disebutkan hanya mewakili beberapa dari banyaknya masalah penyalahgunaan akun oleh pihak ketiga (*hacker*). Melihat pada banyaknya kasus-kasus yang terjadi di dalam penggunaan *paylater*, menunjukkan bahwa konsumen sebagai pengguna layanan transaksi elektronik belum mendapatkan perlindungan hukum. Hal ini dapat dilihat pada beban kerugian yang ditimbulkan dan pertanggungjawaban akibat kasus pembobolan akun kembali dibebankan kepada para korban/pemiliki akun *paylater*. Oleh karena itu, urgensi keamanan transaksi elektronik menjadi suatu hal yang membutuhkan upaya tindaklanjut dari pihak terkait sebagai wujud dalam perlindungan konsumen.

## 2. Metode Penelitian

Penelitian ini adalah penelitian normatif-empiris. Selain mengkaji hukum secara teoretik dan normatif, juga akan mengkaji hukum dalam pelaksanaannya dalam masyarakat.[10] Penelitian dilakukan di Kota Makassar, yaitu Otoritas Jasa Keuangan Regional 6 dan pada beberapa perusahaan aplikasi belanja online yang menyediakan layanan *paylater*, seperti PT. Trinusa Travelindo (Traveloka), PT. Aplikasi Karya Anak Bangsa (Gojek), dan PT. Shopee International Indonesia (Shopee). Data yang diperoleh melalui kegiatan, diidentifikasi dan dikelompokkan menurut karakteristik tujuan penelitian, kemudian di analisis secara kualitatif deskriptif.

## 3. Perlindungan Hukum terhadap Konsumen atas Penyalahgunaan Fitur Kredit (*Paylater*)

Perkembangan pesat dunia e-commerce dewasa ini ditunjukkan salah satunya berdasarkan data yang dipublikasikan oleh Bank Indonesia yang menunjukkan adanya kenaikan dalam transaksi toko online (*e-commerce*) di Indonesia secara drastis yang dapat dilihat pada Tabel 1. nilai transaksi belanja *online* mengalami kenaikan di tahun 2020, yakni sebesar Rp. 429 Trilliun dibandingkan tahun lalu yang mencapai Rp. 201 Trilliun Hal ini dipengaruhi oleh peningkatan jumlah pengguna internet di Indonesia, di mana pada tahun 2020 jumlah pengguna Internet di Indonesia telah mencapai 175.400.000 (seratus tujuh puluh lima empat ratus juta) jiwa, pengguna internet melalui *smartphone* sebanyak 338.200.000 (tiga ratus tiga puluh delapan juta dua ratus ribu). Peningkatan jumlah pengguna internet kemudian berdampak pula pada peningkatan

[9] Arlin. *Akun Shopee Paylater Diretas, Kenapa Pihak Konsumen yang Harus Membayar Tagihan?*. https://mediakonsumen.com/2020/09/25/surat-pembaca/akun-shopee-paylater-diretas-kenapa-pihak-konsumen-yang-harus-membayar-tagihan diakses tanggal 16 September 2019.

[10] Irwansyah. 2020. *Penelitian Hukum: Pilihan Metode dan Praktik Penulisan Artikel*. Mirra Buana Media, Yogyakarta, hlm 42.

jumlah konsumen digital, yang pada tahun 2020 ini telah mencapai 137.000.000 (seratus tiga puluh tujuh juta) jiwa.[11]

**Tabel 1.** Data Jumlah Pertumbuhan *E-Commerce* di Indonesia Tahun 2019-2020

| Tahun | Pengguna Internet | Pengguna Internet *Mobile* | Pengguna Aktif Media Sosial | Jumlah Konsumen Digital | Jumlah Transaksi *E-Commerce* |
|---|---|---|---|---|---|
| 2019 | ± 150.000.000 jiwa | ± 323.200.000 jiwa | ± 160.000.000 jiwa | ± 119.000.000 jiwa | Rp. 201 Trilliun |
| 2020 | ± 175.400.000 jiwa | ± 338.200.000 jiwa | ± 172.000.000 jiwa | ± 137.000.000 jiwa | Rp. 429 Trilliun |

*Sumber: Data Sekunder, 2020 (diolah).*

Terjadinya peningkatan jumlah pengguna internet *mobile* di Indonesia yang mencapai 338,2 (tiga ratus tiga puluh delapan koma dua) juta orang berdampak pada peningkatan jumlah transaksi *e-commerce*. Hal ini dikarenakan dengan tersedianya layanan internet pada tiap-tiap ponsel menjadikan masyarakat lebih mudah dalam mengadakan aktivitas mobilisasi termasuk dalam hal mengakses situs-situs belanja *online* melalui aplikasi digital yang dapat diunduh pada setiap *smartphone*. Di dalam aplikasi belanja *online*, konsumen dimanjakan dengan sejumlah fitur dan fasilitas, seperti potongan harga (diskon), hadiah uang tunai atau poin yang diberikan oleh suatu perusahaan setelah konsumen melakukan pembelian barang dan/atau jasa di perusahaan tersebut (*cashback*), dan kemudahan pembayaran dengan berbagai metode yang ditawarkan, seperti cicilan menggunakan kartu kredit atau tanpa kartu kredit, yakni melalui fitur pembayaran berkala/bayar kemudian (*paylater*).

Berdasarkan riset yang dilakukan oleh Kredivo sebagai salah satu perusahaan *Peer to Peer Lending*, peningkatan jumlah transaksi *e-commerce* yang terjadi pada tahun 2019-2020 juga selain dipengaruhi oleh bertambahnya jumlah konsumen *e-commerce* juga dipengaruhi oleh adanya kolaborasi antara perusahaan *peer to peer lending* dengan perusahaan *e-commerce* dalam peluncuran opsi pembayaran berkala (*paylater*).[12] Meskipun belum ada data yang spesifik mengenai jumlah pengguna *paylater*, namun berdasarkan laporan dari Fintech Report 2019 yang dirilis *DSResearch*, keberadaaan *paylater* (56,7%) saat ini telah menjadi layanan favorit peringkat ketiga setelah dompet digital (82,7%), dan aplikasi investasi (62,4%).[13] Salah satu faktornya adalah karena layanan *paylater* dapat digunakan dalam pembayaran produk *e-commerce*.

*Paylater* adalah fasilitas keuangan dari perusahaan belanja *online* yang memungkinkan metode pembayaran dengan cicilan tanpa kartu kredit atau yang umum dikenal dengan kredit *online*. Melalui layanan *paylater*, dapat memberikan kemudahan kepada konsumen untuk membeli barang dan/atau jasa yang dikehendakinya tanpa perlu membayar dulu. Proses pendaftaran *paylater* umumnya kebih mudah dan cepat

[11] Graha Nurdian, *E-Commerce Indonesia Tahun 2020. Era Digital Mendominasi,* dikutip pada laman website: *https://grahanurdian.com/e-commerce-indonesia-tahun-2020/#1.* diakses tanggal 16 November 2020.

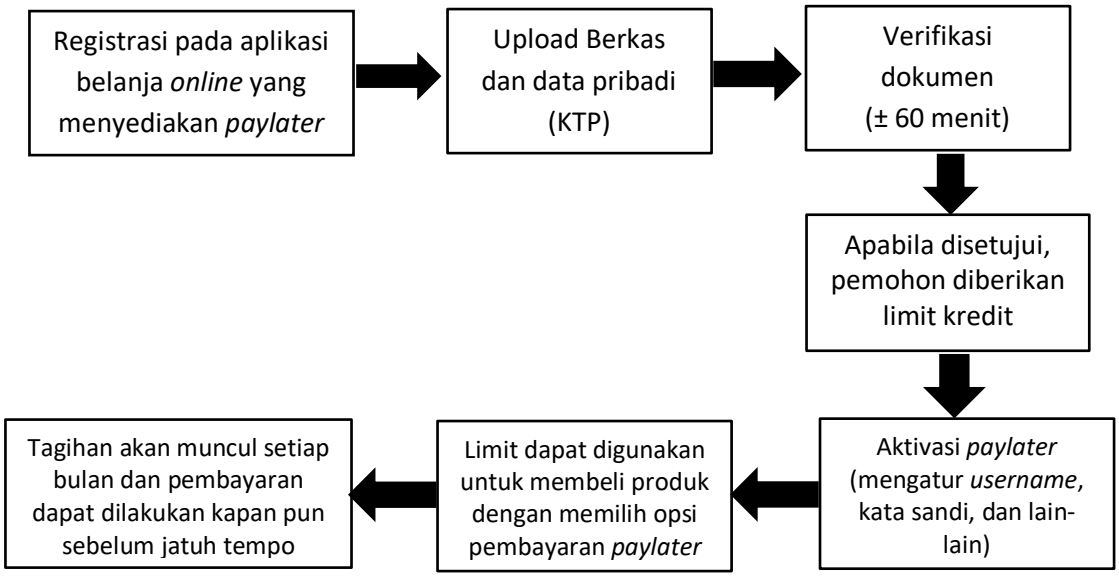
[12] Prasetyo Herfianto, Riset Kredivo: Opsi Pembayaran Berkala Tingkatkan Transaksi di E-Commerce, https://gizmologi.id/insight/riset-kredivo-transaksi-ecommerce, diakses tanggal 18 Desember 2020.

[13] Fintech Reports, 2019. *Moving Towards a New Era in Indonesia's Financial Industry*. DSResearch, Indonesia diakses dalam https://dailysocial.id/post/fintech-report-2019 tanggal 18 Desember 2020.

dibandingkan dengan kartu kredit, serta tidak ada biaya tambahan, seperti biaya tahunan dan uang muka.[14]

Di dalam penggunaan layanan *paylater*, setiap konsumen diwajibkan untuk melakukan registrasi terlebih dahulu pada halaman aplikasi belanja *online* yang menyediakan fasilitas pembayaran *paylater* tersebut serta wajib memenuhi syarat dan ketentuan yang tetapkan, seperti yang pada umumnya wajib memiliki Kartu Tanda Penduduk (KTP) dan domisili yang sah, dan berusia antara 21 – 70 (dua puluh satu sampai dengan tujuh puluh) tahun. Setelah syarat terpenuhi serta pendaftaran telah diverifikasi dan disetujui, pengguna akan diberikan limit hingga Rp. 50.000.000,- (lima puluh juta rupiah). Selanjutnya, pembayaran pinjaman *paylater* akan ditagihkan per 30 (tiga puluh) hari setelah transaksi, atau menggunakan cicilan dengan skema 1 (satu) bulan hingga 12 (dua belas) bulan (Bagan 1).

**Bagan 1.** Alur Penggunaan *Paylater*




*Sumber : Data primer, 2020.*

Berdasarkan penjelasan tersebut di atas terkait dengan alur penggunaan *paylater*, menunjukkan bahwa dengan melakukan registrasi layanan *paylater* dan ketika permohonan disetujui maka secara hukum penggunanya terikat pada suatu hubungan kontraktual dengan penyedia layanan pembayaran *paylater*. Hubungan kontraktual yang dimaksud adalah lahirnya perjanjian penggunaan layanan di antara pengguna jasa dengan penyedia layanan *paylater* dalam bentuk kontrak elektronik sebagaimana didasarkan pada Pasal 1 angka 17 UU ITE bahwa "kontrak elektronik adalah perjanjian para pihak yang dibuat melalui sistem elektronik."

[14] Wawancara tidak langsung dengan Deo selaku *Manager Product* Traveloka, tanggal 15 Oktober 2020.

Lahirnya kontrak elektronik tidak terlepas dari Pasal 1313 BW bahwa "perjanjian adalah suatu perbuatan dengan nama satu orang atau lebih mengikat dirinya terhadap satu orang atau lebih." Selanjutnya, dalam Pasal 1320 KUHPerdata suatu perjanjian dikatakan sah apabila memenuhi 4 (empat) syarat, yaitu kata sepakat dari mereka yang mengikat dirinya; kecakapan untuk membuat suatu perikatan; suatu hal tertentu; dan sebab yang halal.

Perwujudan kata sepakat dalam perjanjian penggunaan layanan *paylater* adalah pada saat registrasi di mana pengguna jasa membubuhkan tanda centang pada halaman registrasi sebagai tanda pernyataan bahwa pengguna jasa telah menyetujui segala ketentuan yang berkaitan *paylater*. Adapun mengenai syarat kecakapan terwujud ketika pengguna jasa telah dinyatakan lolos verifikasi berdasarkan KTP yang dilampirkan karena telah memenuhi syarat usia yang tetapkan oleh pengguna jasa, yakni antara antara 21 – 70 (dua puluh satu sampai dengan tujuh puluh) tahun.

Selanjutnya, suatu hal tertentu telah terpenuhi ketika pengguna jasa telah menyetujui hak-hak dan kewajiban yang timbul atas penggunaan layanan *paylater*, yang tidak terbatas pada kebijakan penggunaan *paylater* yang telah ditentukan oleh pihak penyedia jasa, seperti mengenai biaya tambahan yang timbul, cara pembayaran dan penagihan, syarat keamanan, privasi data pribadi pengguna jasa, dan lain sebagainya.[15] Sedangkan, suatu sebab yang halal dianggap terpenuhi dalam perjanjian penggunaan layanan *paylater* sepanjang isi perjanjian tersebut tidak bertentangan dengan peraturan perundang-undangan yang berlaku.

Di dalam penggunaan fitur *paylater,* maka di antara pengguna jasa dan penyedia jasa kemudian melahirkan suatu perikatan utang piutang/kredit sebagaimana tunduk pada Kitab Undang-Undang Perdata (BW), sehingga dapat disimpulkan bahwa perjanjian penggunaan fitur *paylater* pada suatu aplikasi belanja *online* melahirkan sebuah perjanjian kredit. Hal ini menunjukkan bahwa perjanjian utang piutang yang timbul merupakan perjanjian yang sifatnya *accessoir* (perjanjian yang bersifat tambahan) yang lahir karena adanya perjanjian pokok, yakni perjanjian elektronik mengenai penggunaan fitur *paylater*. Muhammad Djumhana menyatakan bahwa perjanjian kredit pada hakikatnya adalah perjanjian pinjam pengganti sebagaimana yang diatur di dalam Pasal 1754 BW, yang menyebutkan bahwa :[16]

> *Perjanjian pinjam pengganti adalah persetujuan dengan mana pihak yang satu memberikan kepada pihak yang lain suatu jumlah tertentu barang-barang yang menghabis karena pemakaian, dengan syarat bahwa pihak yang belakangan ini akan mengembalikan sejumlah yang sama dari macam dan keadaan yang sama pula.*

Perjanjian utang piutang yang lahir sebagaimana dengan sistem bekerjanya *paylater* yakni konsumen yang melakukan pembelian barang dan/atau jasa pada aplikasi belanja *online* terlebih dahulu dibayarkan oleh layanan *paylater*. Dalam tempo 30 (tiga puluh hari) hari sejak tanggal transaksi, pihak penyedia jasa *paylater* akan melakukan penagihan kembali kepada konsumen sesuai dengan total pembelanjaan yang dilakukan ataupun tagihan berdasarkan jumlah cicilan setiap bulannya, baik dengan tenor 1 (satu) bulan hingga 12 (dua belas) bulan.

---

[15] Khairul Wafa. (2020). "Tinjauan Hukum Ekonomi Syariah terhadap Shopeepay Later." *Jurnal Hukum Ekonomi Syariah,* Vol. 4, No. 1: 16-30.

[16] Muhammad Djumhana, 2000. *Hukum Perbankan di Indonesia*, Cetakan ketiga, Citra Aditya Bakti, Bandung. Hlm. 385

Merujuk pada kedudukan perusahaan aplikasi belanja *online* sebagai penyedia layanan *paylater*, penyaluran pinjaman melalui layanan *paylater* pada dasarnya lahir berdasarkan perjanjian kerja sama kemitraan antara perusahaan belanja *online* dengan perusahaan pinjaman *online* berbasis *financial technology (peer to peer lending)*. Perusahaan *financial technology (peer to peer lending)* adalah sebuah lembaga keuangan non-bank yang menyalurkan pinjaman secara *online* dan berada di bawah pengawasan Otoritas Jasa keuangan (OJK) sebagaimana telah diatur dalam Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi.[17]

Pada perusahaan *financial technology (peer to peer lending),* maka dana-dana investor yang telah terhimpun kemudian dikelola oleh perusahaan *P2P lending* di mana ia bergabung, dan kemudian disalurkan kembali kepada calon peminjam yang membutuhkan dana. Dalam kaitannya dengan perjanjian kerjasama kemitraan antara perusahaan belanja *online* dengan perusahaan pinjaman *online* berbasis *financial technology (P2P Lending),* maka dana investor tersebut kemudian disalurkan kepada pengguna jasa *paylater*. Sebagai contohnya, pada Traveloka, kehadiran layanan/ fitur *paylater* terlebih dahulu dilandasi oleh perjanjian kerja sama kemitraan dengan PT. Pasar Dana Pinjaman (Danamas) dan PT. Caturnusa Sejahtera Finance. Perjanjian kerja sama kemitraan yang dimaksud adalah PT. Pasar Dana Pinjaman (Danamas) dan PT. Caturnusa Sejahtera Finance adalah selaku pihak pemberi pinjaman, sedangkan pihak Traveloka adalah pihak penyalur pinjaman.[18]

Adanya jaminan perlindungan hukum bagi pengguna jasa *paylater* maka memberikan kewajiban bagi perusahaan aplikasi belanja *online* sebagai penyedia fitur *paylater* yang berdasarkan UU ITE sebagai penyelenggara sistem elektronik[19] untuk bertanggung jawab terhadap beroperasinya sistem elektronik,[20] khususnya terhadap perlindungan terhadap data pribadi nasabah yang merupakan suatu hal yang wajib menjadi prioritas utama. Tujuannya tidak lain adalah untuk mencegah timbulnya permasalahan mengenai penyalahgunaan informasi data pribadi pengguna jasa yang berujung pada timbulnya kerugian. Hal ini wajib dilakukan khususnya oleh penyedia jasa maupun perusahaan *P2P Lending* yang bekerja sama mengingat adanya data-data pribadi pengguna jasa yang diunggah pada saat melakukan registrasi *paylater* sebagaimana yang diuraikan dalam Bagan 1 yang wajib dijaga kerahasiannya sebagai wujud keamanan dalam transaksi melalui aplikasi belanja *online* dengan pembayaran menggunakan fitur *paylater.*

Kasus pembobolan akun yang pernah dialami oleh para responden akibat kebocoran data pribadi ternyata tidak hanya dijumpai pada sebuah aplikasi belanja *online* yang menyediakan jasa *paylater*, melainkan kasus pembobolan akun *paylater* telah menyebar

---

[17] Pasal 1 angka 3 Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi : Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi adalah penyelenggaraan layanan jasa keuangan untuk mempertemukan pemberi pinjaman dengan penerima pinjaman dalam rangka melakukan perjanjian pinjam meminjam dalam mata uang rupiah secara langsung melalui sistem elektronik dengan menggunakan jaringan internet.

[18] Wawancara tidak langsung dengan Deo selaku Manager Product Traveloka, tanggal 15 Oktober 2020.

[19] Pasal 1 angka 6 a UU ITE : Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara Negara, Badan Usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik, baik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.

[20] Pasal 3 PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

pada beberapa aplikasi belanja *online*. Adapun tanggapan responden berkenaan dengan hal tersebut dapat diuraikan sebagai berikut :

**Tabel 2.** Tanggapan Responden Mengenai Aplikasi Terjadinya Kasus Pembobolan Akun *Paylater*

| No. | Aplikasi Belanja *Online* | Jumlah | Persentase |
|---|---|---|---|
| 1. | Traveloka | 10 | 50 % |
| 2. | Go-Jek | 4 | 20% |
| 3. | Shopeepay Later | 6 | 30 % |
| | **Jumlah** | 20 | 100 % |

*Sumber: Data Primer, Diolah, 2020.*

Merujuk pada Pasal 2 ayat (5) huruf b PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, keberadaan Traveloka, Go-Jek, dan Shopee adalah termasuk sebagai penyelenggara sistem elektonik lingkup privat. Hal ini ditentukan melihat layanan yang diberikan oleh Traveloka, Go-Jek, dan *Shopee* adalah menyediakan, mengelola, dan/atau mengoperasikan penawaran dan/atau perdagangan barang dan/atau jasa; serta menyediakan, mengelola, dan/atau mengoperasikan layanan transaksi keuangan.

Traveloka dikenal sebagai perusahaan yang menyediakan akomodasi tiket pesawat, hotel, ketera api, bus, mobil dan aktivitas wisata; Go-Jek yang awalnya terkenal sebagai aplikasi yang menyediakan jasa ojek *online* pertama di Indonesia yang saat ini telah mengembangkan fitur layanannya (*Go-food, Go-Mart, Go-Shop, Go-Clean*, dan lain sebagainya); serta *Shopee* yang merupakan perusahaan asal Singapura yang telah melebarkan usahanya di Indonesia yang menyediakan layanan *platform* jual beli *online* menawarkan berbagai macam produk barang dan/atau jasa yang saat ini semakin digemari oleh kaum milenial. Selanjutnya, pada ketiga aplikasi belanja *online* tersebut juga menyediakan layanan transaksi keuangan seperti transaksi pembayaran *online* berupa debit *online*, kartu kredit, transfer rekening, *paylater*, dan opsi-opsi pembayaran tersedia lainnya.

Seiring dengan perkembangannya, keberadaan aplikasi-aplikasi belanja *online* tersebut menjadi incaran para peretas dunia maya (*hacker*) untuk meraup keuntungan dengan cara melawan hukum, yaitu membobol akun para pengguna *paylater* dan kemudian digunakan disalahgunakan dengan melakukan pembelanjaan untuk keperluan pribadi mereka. Beberapa penyebab terjadinya kasus pembobolan akun *paylater* berdasarkan keterangan para responden disebabkan oleh beberapa faktor:

1. Pengguna *paylater* sebelumnya tidak menyadari bahwa *e-mail* telah diretas sehingga para *hacker* mendapatkan akses *paylater* dari *e-mail* yang telah diretas tersebut;
2. Adanya kemungkinan kebocoran data pribadi pengguna *paylater* akibat kurang memadainya pengamanan sistem elektronik yang disediakan oleh penyedia jasa;
3. Pengguna *paylater* pada umumnya memasukkan kata sandi yang mudah ditebak, seperti tanggal/bulan/tahun kelahiran;

4. Pengguna *paylater* karena keteledorannya atau tanpa sadar memberitahukan kata sandi ataupun *one time password* (OTP) yang dikirimkan melalui via SMS dari pihak penyedia jasa kepada pihak yang tidak dikenal, baik melalui *spam call*, yakni adanya telepon yang diterima dari pihak yang tidak dikenal yang mengatasnamakan pihak penyedia jasa *paylater*, ataupun mengaku dari pihak yang mengatasnamakan bank, bahkan ada yang mengaku sebagai polisi.

Selain beberapa penyebab kasus pembobolan akun di atas, di dalam wawancara dengan Adi Darmawan selaku aparat kepolisian Tim Siber Pada Polda Sulsel menambahkan bahwa penyebab lain kebocoran data pribadi yang pernah diperoleh berdasarkan hasil penyelidikan adalah melalui modus *social engineering* yang dilakukan oleh pelaku, yakni dengan cara mencuri informasi langsung dari mulut pengguna. Melalui hubungan sosial seperti melalui obrolan, *hacker* berupaya mengorek informasi yang dibutuhkan.[21]

Kasus pembobolan akun *paylater* yang marak terjadi seiring dengan gencarnya aktivitas jual beli secara *online* perlu mendapatkan perhatian dari pemerintah dan aparatur kepolisian, disamping bagi penyedia jasa juga wajib untuk selalu meningkatkan keamanan dalam menyelenggarakan sistem elektroniknya. Dikatakan demikian, karena jika kasus pembobolan akun *paylater* terus terjadi dan tidak ditangani akan menghilangkan rasa kepercayaan dari masyarakat terhadap sistem keamanan dalam lalu lintas pembayaran elektronik di Indonesia, terlebih menimbulkan bumerang bagi pemerintah mengenai lemahnya undang-undang yang mengatur mengenai keamanan dalam transaksi elektronik, yakni UU Nomor 19 Tahun 2016 tentang Perubahan Atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Ditemukan bahwa pertimbangan beberapa responden yang menyatakan tidak melaporkan kasus pembobolan tersebut kepada aparat kepolisian karena lambatnya proses penindakan yang dilakukan; serta sangat kecil kemungkinan mendapatkan kembali pengembalian atas kerugian materil yang dialami karena dalam pelaku kejahatan dunia maya sulit ditemukan.[22] Tanggapan lain diperoleh salah satu responden, yaitu MY yang melaporkan kasus yang dialaminya kepada aparat kepolisian setempat menyatakan bahwa tidak diperoleh tindak lanjut dari aparat kepolisian mengenai laporan yang disampaikan karena aparat kepolisian tidak berhasil menangkap pelaku.[23]

Tim Siber Polda Sulawesi Selatan, Adi Darmawan, menjelaskan bahwa di dalam menindaki kasus ilegal akses, pihaknya yang menerima laporan dari masyarakat melakukan penyelidikan dan kemudian dilakukan analisa dari data atau dokumen yang diberikan korban agar dapat dijadikan sebagai petunjuk guna melengkapi kasus tersebut. Beberapa metode penyelidikan yang dilakukan oleh Direktorat Reserse Kriminal Khusus Subdit Cyber Polda Sulawesi Selatan adalah mulai dari observasi, penelitian data atau dokumen, penyamaran dan pelacakan, serta upaya-upaya penuh

[21] Wawancara dengan Adi Darmawan selaku BANIT SUBDIT 5 Tindak Pidana Siber DITRESKRIMSUS pada Polda Sulawesi Selatan, tanggal 16 Oktober 2020.

[22] Tanggapan dari 4 (empat) responden yang dirangkum.

[23] Tanggapan dari MY salah satu responden/korban pembobolan akun Traveloka *Paylater*.

lainnya guna untuk mendapatkan petunjuk ataupun barang bukti dalam sebuah kejahatan tindak pidana siber.[24]

Terkait dengan tanggapan dari salah satu responden yang menyatakan tidak melaporkan kasus tersebut kepada aparat kepolisian diakibatkan lambatnya proses penindakan yang dilakukan, Adi Darmawan menanggapi bahwa sesuai dengan Peraturan Kepala Kepolisian Negara Republik Indonesia Nomor 6 Tahun 2019 tentang Penyidikan Tindak Pidana, dikarenakan kasus pembobolan akun termasuk dalam kasus sulit, maka waktu yang dibutuhkan untuk dilakukan penyelidikan adalah kurang lebih sekitar 30 (tiga puluh) hari. Selanjutnya, apabila belum ditemukan titik terang dari pelaku kejahatan, hasil pelaksanaan dari proses penyelidikan dilakukan Gelar Perkara bersama atasan mereka untuk menentukan apakah kasus tersebut ditindakjanjuti atau dihentikan. Adapun kesulitan di dalam melakukan penyelidikan tindak pidana *hacking* adalah ketika para pelaku menghilangkan jejak digital dalam melakukan kejahatannya. [25]

Berkenaan dengan penjelasan di atas, penulis berpendapat bahwa mengingat kasus pembobolan akun dalam transaksi elektronik termasuk ke dalam jenis kasus yang sulit untuk menangkap pelaku kejahatan dikarenakan pelaku melakukan aksinya tidak secara terang-terangan atau dengan kata lain melalui dunia maya, maka daripada itu tindakan pencegahan (preventif) berupa perlindungan data pribadi secara andal dan memadai wajib diterapkan oleh penyelenggara sistem elektronik untuk mencegah peningkatan kasus pembobolan akun.

Permasalahan kerugian yang timbul akibat kasus pembobolan akun sebagaimana tetap dibebankan kepada para pengguna jasa merupakan pembebasan tanggung jawab penyedia jasa yang pada umumnya telah ditentukan secara sepihak di dalam perjanjian elektronik yang telah sepakati di awal pendaftaran fitur *paylater*. Sebagaimana halnya Traveloka, telah ditentukan pada syarat dan ketentuan penggunaan Traveloka *Paylater* yang berisi klausula bahwa:

> *Kami tidak bertanggung jawab atas kerugian, beban, biaya (termasuk pengeluaran dan biaya hukum), ganti rugi, atau denda yang ditimbulkan (terlepas dari bentuk tindakan) yang timbul, secara langsung atau tidak langsung, sehubungan dengan :*
> *Keterbatasan akses, penggunaan dan/atau ketidakmampuan Anda untuk menggunakan Traveloka PayLater termasuk namun tidak terbatas pada hal berikut:*
> 1. *Jika Anda tidak memiliki cukup saldo atau batas kredit yang tersedia di akun Traveloka PayLater Anda untuk melakukan pembelian;*
> 2. ***Jika akun Traveloka PayLater Anda telah disusupi**, atau jika kami memiliki alasan untuk percaya bahwa akun Traveloka PayLater Anda telah disusupi;*
> 3. *Jika informasi transaksi yang diberikan oleh Anda atau pihak ketiga tidak benar;*
> 4. *Jika keadaan di luar kendali kami (force majeure) yang mencegah transaksi Anda;*

[24] Wawancara dengan Adi Darmawan selaku BANIT SUBDIT 5 Tindak Pidana Siber DITRESKRIMSUS pada Polda Sulawesi Selatan, tanggal 16 Oktober 2020.

[25] Wawancara dengan Adi Darmawan selaku BANIT SUBDIT 5 Tindak Pidana Siber DITRESKRIMUS pada Polda Sulawesi Selatan, tanggal 16 Oktober 2020.

Kebijakan tersebut juga ditetapkan pada Shopee sebagaimana diuraikan dalam kebijakan privasinya yang salah satu di antaranya menyatakan sebagai berikut : [26]

> *Kami tidak bertanggung jawab maupun memper-tanggungjawabkan konten, pengaturan keamanan (atau tidak adanya pengaturan keamanan), dan aktivitas situs-situs terkait ini. Situs-situs yang terkait ini hanya untuk kenyamanan Anda, dan oleh karenanya Anda mengaksesnya atas risiko Anda sendiri. Namun begitu, kami berupaya melindungi integritas Platform kami dan tautan yang ditempatkan pada masing-masing situs, dan oleh karena itu, kami menyambut setiap umpan-balik mengenai situs-situs yang tertaut ini.*

Menurut hemat penulis, kerugian materil yang timbul akibat pembobolan akun tidak semestinya secara serta merta langsung dibebankan kepada korban. Pihak penyelenggara sistem elektronik seharusnya terlebih dahulu melakukan penyelidikan terkait dengan kasus pembobolan akun yang terjadi, apakah disebabkan oleh keteledoran dari pengguna jasa yang tanpa sadar membocorkan sendiri informasi pribadi yang terdapat pada aplikasi belanja *online,* ataukah pembobolan akun *paylater* disebabkan oleh kelalaian pihak penyedia jasa, seperti lemahnya sistem elektronik dari penyedia jasa sehingga menjadi celah bagi *hacker* untuk memeroleh data pribadi pengguna jasa *paylater*.

Jika kasus pembobolan akun disebabkan karena pengguna jasa sendiri yang menginformasikan beberapa informasi pribadi (baik disadari maupun tidak disadari) sehingga menyebabkan kebocoran data pribadi, maka beban kerugian dapat dibebankan kepada pengguna jasa. Hal ini sebagaimana telah ditentukan di dalam Pasal 3 ayat (3) PP Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang menentukan bahwa penyelenggara sistem elektronik tidak bertanggungjawb terhadap beroperasinya sistem elektronik dalam hal dapat dibuktikan terjadinya keadaan memaksa, kesalahan, dan/atau kelalaian pihak Pengguna Sistem Elektronik.

Bagi responden yang memutuskan untuk tetap menggunakan *paylater* adalah karena mereka telah mengubah dan memperketat sistem keamanan pada aplikasi belanja *online* mereka seperti dengan mengaktifkan sistem keamanan berlapis, sistem autentikasi biometrik pada ponsel masing-masing yang diperlukan pada saat akan melakukan transaksi, sehingga mereka merasa bahwa dengan memperketat sistem keamanan tersebut akan sulit bagi *hacker* untuk kembali melakukan pembobolan akun.[27]

Berdasarkan hal-hal yang telah diuraikan di atas, dapat disimpulkan bahwa maraknya kasus pembobolan akun *paylater* telah terjadi pada beberapa aplikasi belanja *online* yang menyediakan layanan *paylater* dipicu karena adanya kebocoran data pribadi yang tersimpan pada aplikasi belanjan *online* tersebut. Terhadap kerugian materil yang ditimbulkan, tetap dipikulkan kepada korban tanpa dilakukan penyelidikan pasti mengenai penyebab terjadinya kasus pembobolan akun, dimana hal tersebut pada umumnya dijelaskan oleh pihak penyelenggara sistem elektronik pada kebijakan privasi penggunaan layanan. Mengenai peranan aparat kepolisian dalam hal ini masih tergolong pasif akibat masih kurangnya korban yang melaporkan kasus pembobolan akun *paylater* yang dialaminya. Oleh karena itu, berdasarkan fenomena yang ada

[26] Shopee, Kebijakan Privasi, https://shopee.co.id/docs/3612, diakses tanggal 19 November 2020.
[27] Tanggapan dari RR selaku responden yang menyatakan

menunjukkan bahwa langkah antisipatif berupa peningkatan sistem keamanan elektronik sudah sepantasnya dibangun oleh para penyelenggara sistem elektronik guna untuk mencegah serta meminimalisir terjadinya kasus pembobolan akun *paylater*.

## 4. Pengawasan Otoritas Jasa Keuangan (OJK) Terkait dengan Perlindungan Hukum Atas Penyahgunaan Akun Paylater oleh Pihak Ketiga

Otoritas jasa keuangan (OJK) adalah lembaga negara yang dibentuk berdasarkan Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan yang menyelenggarakan fungsi pengaturan dan pengawasan yang terintegrasi terhadap keseluruhan kegiatan di dalam sektor jasa keuangan baik di dalam sektor jasa keuangan baik di sektor perbankan, pasar modal, dan sektor jasa keuangan non bank seperti asuransi, dana pensiun, lembaga pembiayaan, dan lembaga jasa keuangan lainnya. Terkait dengan keberadaannya dalam melakukan pengawasan pada sektor non perbankan, maka OJK juga berwenang untuk melakukan pengawasan terhadap perusahaan *financial technology peer to peer lending* (*P2P Lending*) yang saat ini tengah banyak menjalin kerja sama kemitraan dengan perusahaan aplikasi belanja *online* dalam menyediakan fitur *paylater*.

Berdasarkan wawancara yang dilakukan dengan Normasita selaku Kepala Sub Bagian *Financial Techologi P2P Lending* pada Otoritas Jasa Keuangan Kantor Regional 6 Kota Makassar, menjelaskan bahwa legalitas OJK di dalam melakukan pengawasan diatur di dalam POJK Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Berbasis Teknologi Informasi.[28] Merujuk pada Pasal 28 POJK Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Berbasis Teknologi Informasi telah ditentukan beberapa standar keamanan yang wajib diterapkan oleh seluruh perusahaan *fintech P2P Lending* baik yang dalam kedudukannya sebagai penyelenggara sistem elektronik maupun yang bekerja sama dengan penyelenggara sistem elektronik lainnya khususnya yang menfasilitasi pembayaran digital, antara lain sebagai berikut :

(1) Penyelenggara wajib melakukan pengamanan terhadap komponen sistem teknologi informasi dengan memiliki dan menjalankan prosedur dan sarana untuk pengamanan Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi dalam menghindari gangguan, kegagalan, dan kerugian.
(2) Penyelenggara wajib menyediakan sistem pengamanan yang mencakup prosedur, sistem pencegahan, dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian.
(3) Penyelenggara wajib ikut serta dalam pengelolaan celah keamanan teknologi informasi dalam mendukung keamanan informasi di dalam industri layanan jasa keuangan berbasis teknologi informasi.
(4) Penyelenggara wajib menampilkan kembali Dokumen Elektronik secara utuh sesuai dengan format dan masa retensi yang ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Berdasarkan ketentuan di atas, dapat diketahui bahwa kewajiban untuk menjaga sistem keamanan di dalam transaksi elektronik tidak hanya menjadi kewajiban perusahaan aplikasi *e-commerce* yang mendukung fitur pembayaran *paylater*, melainkan berdasarkan POJK Nomor 77/POJK.01/2016 tentang Layanan Pinjam

[28] Wawancara dengan Normasita selaku Kepala Sub Bagian *Financial Techologi P2P Lending* pada Otoritas Jasa Keuangan Kantor Regional 6 Kota Makassar, tanggal 13 Novembr 2020.

Meminjam Berbasis Teknologi Informasi, maka kewajiban untuk menjaga sistem keamanan transaksi elektronik juga ditekankan kepada perusahaan *financial technologi* (*P2P Lending*) yang bekerja sama dengan perusahaan aplikasi belanja *online*. Normasita menjelaskan bahwa adanya kewajiban untuk menjaga sistem keamanan transaksi mengingat dana pinjaman yang disalurkan melalui fitur *paylater* pada aplikasi belanja *online* berasal dari dana-dana investor sehingga pengembaliannya wajib dijamin oleh perusahaan *financial technology* (*P2P Lending*) sebagai pengelola dana. Oleh karena itu, apabila kasus pembobolan akun paylater terus terjadi pada aplikasi belanja *online* yang bekerja sama dan merugikan perusahaan *financial technology* (*P2P Lending*) akibat korban pembobolan akun tidak mau membayar tagihan yang timbul, maka akan berdampak pada kerugian investor yang selanjutnya akan menghilangkan kepercayaan pihak-pihak investor dalam menginvestasikan dananya pada perusahaan *financial technology* (*P2P Lending*).

Kewajiban untuk menjaga keamanan sistem sebagaimana diterapkan OJK sebagaimana telah ditentukan di dalam Pasal 29 POJK Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Berbasis Teknologi Informasi, salah satunya adalah melalui penerapan prinsip dasar perlindungan pengguna dengan mewajibkan para perusahaan *financial technology (P2P Lending*) untuk menjaga kerahasiaan dan keamanan data dan informasi pribadi pengguna *paylater* yang diperoleh/diteruskan dari perusahaan aplikasi belanja *online* yang bekerja sama. Apabila ketentuan tersebut dilanggar dan berdasarkan hasil investigasi ditemukan bahwa kebocoran data pribadi pengguna jasa berasal dari sistem keamanan perusahaan *financial technology* (*P2P Lending*) yang kurang memadai, maka OJK akan memberikan sanksi teguran kepada perusahaan *financial technology* (*P2P Lending*). [29]

Menurut Bondan, Staf Bagian *Financial Techologi P2P Lending* pada Otoritas Jasa Keuangan Kantor Regional 6 Kota Makassar diperoleh penjelasan lebih lanjut bahwa upaya perlindungan hukum lain yang diterapkan oleh OJK guna mencegah terjadinya kasus pembobolan akun dalam transaksi elektronik termasuk pada pembayaran menggunakan fitur *paylater* adalah dengan melakukan edukasi kepada masyarakat. Pemberian edukasi telah disampaikan melalui media sosial, radio, televisi, maupun pemberitaan pada media cetak. Edukasi tersebut ditujukan agar pengguna jasa menjadi lebih paham dan cerdas, yakni lebih cepat mengenali modus penipuan maupun *social engineering* yang dilakukan oleh para para peretas untuk mengorek informasi calon korban. Selain itu, pengguna jasa juga telah dihimbau untuk menjaga keamanan akun dan informasi pribadi yang dimasukkan di dalam aplikasi belanja *online* tersebut.

Berdasarkan hal-hal yang telah diuraikan di atas dapat disimpulkan bahwa perlindungan hukum terhadap konsumen sebagai pengguna jasa *paylater* atas penyalahgunaan fitur *paylater* pada aplikasi belanja *online* telah diterapkan oleh perusahaan aplikasi belanja *online* sebagai penyelenggara sistem elektronik dan Otoritas Jasa Keuangan melalui pengawasan dan kewajiban penerapan prinsip dasar perlindungan pengguna kepada perusahaan *financial technology (P2P Lending)* yang bekerja sama dengan perusahaan aplikasi belanja online dalam menyediakan fitur *paylater*. Adapun perlindungan hukum yang dimaksud lebih mengarah kepada upaya perlindungan hukum preventif yang tujuannya adalah untuk mencegah terjadinya

[29] Wawancara dengan Bondan selaku Staf Bagian *Financial Techologi P2P Lending* pada Otoritas Jasa Keuangan Kantor Regional 6 Kota Makassar tanggal 13 November 2020.

kasus kebocoran informasi data pribadi, sebagaimana yang pada umumnya diterapkan oleh penyelenggara sistem elektronik, antara lain penerapan sistem keamanan berlapis, kerja sama dengan tenaga ahli bersertifikasi, serta edukasi kepada para pengguna jasa. Sedangkan, terhadap kasus pembobolan akun *paylater* yang telah terjadi, ditemukan kendala dari aparat kepolisian dalam menangkap pelaku dan pada umumnya pihak penyelenggara/ penyedia layanan *paylater* tidak bertanggung jawab, sehingga beban kerugian tetap menjadi tanggungan dan dibebankan kepada pengguna jasa.

## 5. Penutup

Perlindungan hukum terhadap konsumen atas penyalahgunaan fitur kredit (*paylater*) oleh pihak ketiga melalui aplikasi belanja *online* telah diterapkan oleh para penyedia jasa fitur *paylater*. Perlindungan hukum berorientasi pada upaya-upaya yang bersifat preventif (pencegahan), seperti bekerja sama dengan lembaga tersertifikasi di dalam menyimpan dan menjaga keamanan data-data/informasi pengguna jasa, menerapkan sistem keamanan berlapis, dan memberikan edukasi kepada para pengguna jasa. Terhadap kasus pembobolan akun *paylater* yang telah terjadi, pada umumnya penyedia jasa tidak bertanggung jawab sebagaimana telah ditegaskan di dalam kebijakan privasi penggunaan layanan, sehingga beban kerugian yang timbul akibat kasus pembobolan akun tetap dipikul oleh konsumen. Hal ini dikarenakan tidak ada jaminan keamanan mutlak yang dapat diberikan oleh penyedia jasa di dalam menghindari aktivitas peretas di dunia maya. Kepada penyedia layanan paylater, hendaknya di dalam menfasilitasi layanan fitur *paylater* harus memiliki sistem penyimpanan data yang terjamin keamanan dan keandalannya serta menerapkan majemen risiko agar dapat mengidentifikasi dan mencegah transaksi *fraud* (penipuan) yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab.

## Referensi

Achmad Ali. 2009. *Menguak Teori Hukum (Legal Theory) dan Teori Peradilan (Judicial Prudence)*. Jakarta: Kencana Prenada Media Group.

Ahmadi Miru dan Sutarman Yodo. 2010. *Hukum Perlindungan Konsumen*. Rajawali Pers. Jakarta.

Arlin. *Akun Shopee Paylater Diretas, Kenapa Pihak Konsumen yang Harus Membayar Tagihan?. https://mediakonsumen.com/2020/09/25/surat-pembaca/akun-shopee-paylater-diretas-kenapa-pihak-konsumen-yang-harus-membayar-tagihan* diakses tanggal 16 September 2019.

Budiharto Ernama & Hendro. (2017). Pengawasan Otoritas Jasa Keuangan Terhadap Financial Technology (Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016). *Diponegoro Law Journal*, Vol. 6, No. 3: 1-12.

Fintech Reports, 2019. *Moving Towards a New Era in Indonesia's Financial Industry*. DSResearch, Indonesia diakses dalam https://dailysocial.id/post/fintech-report-2019 tanggal 18 Desember 2020.

Gojek. *Kebijakan Privasi Gojek*. https://www.gojek.com/privacy-policies/ diakses tanggal 20 November 2020.

Graha Nurdian, *E-Commerce Indonesia Tahun 2020. Era Digital Mendominasi,* dikutip pada laman website: *https://grahanurdian.com/e-commerce-indonesia-tahun-2020/#1*. diakses tanggal 16 November 2020.

Imam Sjahputra, 2010. *Perlindungan Konsumen Dalam Transaksi Elektronik*. Alumni, Bandung.

Irwansyah. 2020. *Penelitian Hukum: Pilihan Metode dan Praktik Penulisan Artikel.* Mirra Buana Media, Yogyakarta.

Khairul Wafa. (2020). "Tinjauan Hukum Ekonomi Syariah terhadap Shopeepay Later." *Jurnal Hukum Ekonomi Syariah,* Vol. 4, No. 1: 16-30.

Meylinda Rachmadanniar. *Paylater Traveloka Dipakai Orang Lain Dan Lagi-Lagi Pelanggan Disalahkan*. https://mediakonsumen.com/2019/03/14/surat-pembaca/paylater-traveloka-dipakai-orang-lain-dan-lagi-lagi-pelanggan-disalahkan diakses tanggal 16 September 2019.

Muhammad Djumhana, 2000. *Hukum Perbankan di Indonesia*, Cetakan ketiga, Citra Aditya Bakti, Bandung.

Ning Rahayu, *Ini Dampak Perkembangan E-Commerce Bagi Indonesia*, https://www.wartaekonomi.co.id/read216033/ini-dampak-perkembangan-e-commerce-bagi-indonesia.html diakses tanggal 2 April 2020.

Prasetyo Herfianto, Riset Kredivo: Opsi Pembayaran Berkala Tingkatkan Transaksi di E-Commerce, https://gizmologi.id/insight/riset-kredivo-transaksi-ecommerce, diakses tanggal 18 Desember 2020.

Sarah Safira Aulianisa. 2020. "Konsep Dan Perbandingan Buy Now, Pay Later Dengan Kredit Perbankan Di Indonesia: Sebuah Keniscayaan Di Era Digital Dan Teknologi." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional,* Vol. 9, no. 2: 183-194.

Shopee. *Bagaimana Shopee Menggunakan dan Melindungi Data Anda.* https://help.shopee.co.id/s/article/Bagaimana-Shopee-menggunakan-dan-melindungi-data-Anda diakses tanggal 18 November 2020.

Traveloka. *Paylater FAQ*. https://www.traveloka.com/id-id/travelokapay /paylater diakses tanggal 17 September 2019.