Regulasi Keamanan Data Pribadi Pengguna pada *E-commerce* di Indonesia

I Kadek Noppi Adi Jaya[1], Ida Ayu Utari Dewi[2]
Program Studi Sistem Informasi
Universitas Hindu Indonesia
Denpasar, Indonesia
iknadijaya@unhi.ac.id, utaridewi@unhi.ac.id

Abstract - ***E-commerce allows fast and low cost transactions without going through a complicated process. Even though in its application there are still many threats to its security, in the future it is hoped that the E-commerce business can continue to grow, of course, in line with the development of security. Until now, there is only a Draft Government Regulation on E-commerce (RPP E-commerce) concerning Amendments to Government Regulation Number 82 of 2012 concerning Implementation of Electronic Systems and Transactions. Personal data security regulations should be considered as one of the most important areas that Indonesia needs. A good regulatory concept should include: principles, rules, processes and institutions. Namely in the form of principles that take into account both national and international developments, the principle of privacy of information on personal data, the principle of fair information, clear definitions of substantial terms being mentioned in regulations and the presence of a supervisory board.***

Keywords : personal data security regulations, e-commerce

I. PENDAHULUAN

Selama beberapa tahun terakhir, perdagangan elektronik mulai berkembang pesat di dunia termasuk Indonesia. Di mana sebagian besar aktivitas transaksi pembayaran dilakukan melalui Internet. Indonesia merupakan salah satu negara yang jumlah pengguna internetnya sangat besar. Menurut data dari APJI (Asosiasi Penyelenggara Jasa Internet pada laporan tahun 2018 melalui survei yang dilakukan pada tahun 2017 diketahui bahwa pengguna internet di Indonesia diperkirakan mengalami peningkatan yang cukup signifikan dari tahun sebelumnya yaitu 132, 7 juta orang (2016) hingga naik sebesar 8% atau sekitar 143,26 juta pengguna dengan porsi pengguna setara dengan 54,68% dari jumlah penduduk di Indonesia secara keseluruhan yang tersebar diberbagai wilayah [1].

Tren digitalisasi di Indonesia semakin cepat pada era pandemi Covid-19, lewat perubahan perilaku masyarakat. Adopsi digital di Indonesia meningkat pesat dan terus mendongkrak aktivitas transaksi digital dalam kegiatan masyarakat dan semakin terakselerasi di era pandemi Covid-19. Direktur Pemberdayaan Informatika, Direktorat Jenderal Aplikasi Informatika Kementerian Kominfo, menyatakan pertumbuhan nilai perdagangan elektronik (*e-commerce*) di Indonesia mencapai 78 persen, tertinggi di dunia (www.kominfo.go.id)

Terlepas dari kenyamanan dan keberadaannya di mana-mana, perkembangan pesat teknologi informasi telah meningkatkan risiko keamanan seperti pencurian identitas di platform *e-commerce*. Penyerang melakukan pencurian identitas dengan menggunakan berbagai cara jahat yang bertujuan untuk mencuri data pribadi korban seperti sandi, alamat email, dan nomor kartu kredit. Informasi yang dicuri dapat diperdagangkan ke pasar gelap online atau digunakan untuk membeli barang atau jasa secara online.

Akan tetapi, dibalik populernya penjualan secara online, banyak pengguna internet yang masih takut dalam melakukan transaksi, baik untuk membeli/customer dan menjual barang di toko-toko virtual, maupun melakukan transaksi keuangan pada sistem Intenet Banking. Resiko dalam melakukan transaksi di Internet sangat tinggi, karena selain beragamnya tujuan pengguna Internet, regulasi yang menaungi keamanan dalam bertransaksi di Internet juga masih belum memadai [2]. Di Indonesia, terutama potensi penjualan yang besar tersebut belum didukung dengan peraturan perundang-undangan yang memadai karena belum ada peraturan yang secara khusus diterbitkan untuk mengatur sektor *E-commerce*. Hingga saat ini, hanya terdapat Rancangan Peraturan Pemerintah tentang *E-commerce* (RPP *E-commerce*) tentang Perubahan atas Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Selama rancangan peraturan tersebut belum disahkan, maka kerangka utama peraturan perundang-undangan terkait kegiatan *e-commerce* masih mengacu pada Undang-Undang No. 11 tahun 2008 tentang Informasi dan Elektronik (UU ITE) [3]. Tulisan ini bertujuan untuk mengatasi kesenjangan ini dengan menyediakan kerangka kerja yang komprehensif regulasi keamanan data pribadi pengguna pada platform *e-commerce* di Indonesia.

II. KAJIAN PUSTAKA

E-commerce

E-commerce adalah aktivitas komersial melalui alat elektronik. Ini didasarkan pada pemrosesan elektronik dan transmisi informasi (teks, video, audio). *E-commerce* melibatkan banyak aktivitas barang dan jasa, pengiriman informasi digital secara elektronik, lelang elektronik, pemasaran langsung ke konsumen. Perdagangan elektronik dapat diterapkan secara luas di bidang-bidang berikut: perdagangan elektronik; transaksi keuangan dalam penyediaan perbankan, penyewaan keuangan, asuransi dan layanan lainnya, investasi, operasi spekulatif dalam mata uang dan sekuritas; pasar jasa lainnya: hotel, pariwisata, pendidikan, konsultasi, pembayaran utilitas, periklanan dan lainnya; antara berbagai bisnis, publik, publik dan institusi lainnya. Perdagangan elektronik, yang biasa dikenal dengan *E-commerce*, adalah perdagangan produk atau jasa menggunakan jaringan komputer, seperti Internet. Perdagangan elektronik mengacu pada teknologi seperti perdagangan seluler, transfer dana elektronik, manajemen rantai pasokan, pemasaran Internet, pemrosesan transaksi online, pertukaran data elektronik (EDI), sistem manajemen inventaris, dan sistem pengumpulan data otomatis [4]. *E-commerce*, adalah pembelian dan penjualan barang dan jasa di Internet. Selain jual beli, banyak orang menggunakan internet sebagai sumber informasi untuk membandingkan harga atau melihat produk terbaru yang ditawarkan sebelum melakukan pembelian secara online atau di toko tradisional [5]. *E-commerce* dapat didefinisikan sebagai otomatisasi prosedur dan operasi bisnis rutin dan transfer ke ruang virtual. Proses ini sangat meningkatkan efisiensi bisnis dan menyederhanakan pekerjaan rutin sehari-hari. Hingga saat ini, diasumsikan bahwa sebagian besar transaksi *e-commerce* dilakukan di seluruh dunia.

Penggolongan *E-commerce* yang umumnya dilakukan ialah berdasarkan sifat transaksinya. Berdasarkan tipe-tipenya dibedakan sebagai berikut [6].

1. Bussiness to Bussines (B2B), adalah model *E-commerce* dimana pelakiu bisnisnya adalah perusahaan, sehingga sehingga proses transaksi dan informasinya adalah antara satu perusahaan dengan perusahaan lainnya. Contoh penerapan model Ecommerce ini adalah beberapa situs E-banking yang melayani transaksi antar perusahaan.
2. Business to costumer (B2C), adalah model *E-commerce* dimana pelaku bisnisnya melibatkan langsung antara penjual (penyedia jasa *E-commerce*) dengan individu (buyers) atau pembeli. Salah satu contoh layanan ini adalah airasia.com
3. Costumer to costumer (C2C), adalah model *E-commerce* dimana perorangan atau individu berinteraksi dan bertransaksi langsung dengan individu lain sebagai pembeli. Konsep *E-commerce* jenis ini banyak digunakan dalam situs onlin auction atau lelang secara online. Salah satu contoh portal E-commerece yang menerapkan konsep C2C ini adalah ebay.com.
4. Costumer to bussines (C2B), adalah model *E-commerce* dimana pelaku bisnis perorangan atau individu melakukan interaksi atau trnsaksi dengan suatu atau beberapa perusahaan. Jenis *E-commerce* seperti ini sangat jarang dilakukan di Indonesia. Contoh portal *E-commerce* yang menerapkan model seperti ini adalah priceline.com.

Data Pribadi Pengguna

Istilah data pribadi menentukan informasi yang memungkinkan untuk mengidentifikasi seseorang secara langsung atau tidak langsung, khususnya dengan mengacu pada nomor identifikasi atau satu atau lebih faktor yang spesifik untuk identitas fisik, fisiologis, mental, ekonomi, budaya atau sosialnya. Setiap operasi atau rangkaian operasi dengan data pribadi (menggunakan cara otomatis atau tidak otomatis) disebut "pemrosesan data pribadi". Prinsip utama pemrosesan data pribadi memerlukan aturan yang kuat untuk perlindungan data pribadi (PDP) [6]. Data pribadi mengacu pada informasi apa pun yang berkaitan dengan suatu data subjek — orang hidup yang diidentifikasi atau dapat diidentifikasi (bukan legal kesatuan). Potongan-potongan informasi yang berbeda, ketika dikumpulkan bersama-sama, dapat mengarah pada identifikasi orang tertentu juga merupakan data pribadi. Misalnya, semua informasi yang diperlukan Science Editing untuk pendaftaran, seperti file pengguna, email, nama, afiliasi dan departemen, gelar, alamat, dan nomor telepon dan faks, termasuk dalam kategori data pribadi. Selain itu, informasi apa pun tentang pengguna terdaftar yang dibuat setelah pendaftaran mereka (misalnya, hasil tinjauan sejawat, keputusan editorial, waktu penyelesaian, dan / atau komentar apa pun pada penulis atau ulasan) juga termasuk dalam definis ini [8]. Data pribadi berarti setiap informasi yang berkaitan dengan orang yang diidentifikasi atau dapat diidentifikasi ('subjek data'); Orang perorangan yang dapat diidentifikasi adalah orang yang dapat diidentifikasi, secara langsung atau tidak langsung, khususnya dengan mengacu pada pengenal seperti nama, nomor identifikasi, data lokasi, pengenal online atau satu atau lebih faktor yang spesifik untuk fisik, fisiologis, identitas genetik, mental, ekonomi, budaya atau sosial dari orang tersebut.

Artinya, data pribadi harus berupa informasi yang berkaitan dengan individu. Individu tersebut harus diidentifikasi atau dapat diidentifikasi baik secara langsung atau tidak langsung dari satu atau lebih pengenal atau dari faktor-faktor khusus individu tersebut.

GDPR (*General Data Protection Regulation*) Inggris mencakup pemrosesan data pribadi dengan dua cara:

1. Data pribadi yang diproses seluruhnya atau sebagian dengan cara otomatis (yaitu, informasi dalam bentuk elektronik)
2. Data pribadi yang diproses secara non-otomatis yang merupakan bagian dari, atau dimaksudkan untuk menjadi bagian dari, 'sistem pengarsipan' (yaitu, informasi manual dalam sistem pengarsipan).

Data pribadi adalah informasi apa pun yang terkait dengan individu hidup yang diidentifikasi atau dapat diidentifikasi. Potongan informasi berbeda, yang dikumpulkan bersama dapat mengarah pada identifikasi orang tertentu, juga merupakan data pribadi. Data pribadi yang telah dihapus identitasnya, dienkripsi, atau disamarkan tetapi dapat digunakan untuk mengidentifikasi kembali seseorang tetap menjadi data pribadi dan berada dalam cakupan GDPR. Data pribadi yang telah dibuat anonim sedemikian rupa sehingga individu tersebut tidak atau tidak lagi dapat diidentifikasi tidak lagi dianggap sebagai data pribadi. Agar data benar-benar dianonimkan, penganoniman harus tidak dapat diubah [9].

Keamanan Data Pribadi di *E-commerce*

E-commerce telah membantu para pengguna internet di seluruh dunia di dalam proses jual beli secara online. Ada banyak sekali pelaku *E-commerce* yang menjadilannya sebagai bisnis (baik produk maupun jasa) dan tentu saja ada banyak konsumen online yang menggunakan layanan-lauanan tersebut. Sebuah layanan yang aman dan nyaman (termasuk juga pada *E-commerce*), akan menumbuhkan kepercayaan konsumen. Kepercayaan konsumen merupakan salah satu modal utama di dalam menuju kesuksesan dari suatu bisnis online berbasiskan *E-commerce*.

Sistem keamanan pada *e-commerce* mencakup beberapa aspek penting yang dijadikan dasar, yaitu aspek-aspek keamanan, macam-macam ancaman, dan solusi dari kekurangan sistem *e-commerce*. Semua aspek penting pada keamanan *e-commerce* sangat berpengaruh terhadap tingkat keamanan pada sistem keamanan *e-commerce* secara keseluruhan [10].

Proses Kriptografi tidak hanya merahasiakan data transaksi tetapi harus memenuhi aspek lainnya yaitu [11]:

1. Authentication, yaitu pengirim pesan harus benar-benar berasal dari pengirim yang bersangkutan.
2. Integrity, yaitu isi pesan harus benar-benar utuh dan tidak diubah oleh orang lain.
3. Nonrepudiation, yaitu pengirim pesan tidak dapat menyangkal bahwa pesan tersebut dikirim oleh yang bersangkutan.
4. Authority, yaitu pesan yang dikirim hanya dapat diubah oleh pihak yang berwenang.

Dua hal yang utama yang harus diperhatikan dalam melakukan transaksi adalah hal apa saja yang dibutuhkan dalam rangka menciptakan keamanan bertransaksi dan metode yang digunakan untuk menciptakan keamanan tersebut. Dimensi keamanan pada *E-commerce* adalah [12]:

1. Autentikasi, pembeli, penjual, dan institusi pembayaran yang terlibat harus dipastikan identitasnya sebagai pihak yang berhak terlibat dalam transaksi tersebut
2. Integritas, jaminan bahwa data dan informasi yang di transfer pada *e-commerce* tetap utuh dan tidak mengalami perubahan
3. non-repudiation, pelanggan membutuhkan perlindungan terhadap penyangkalan dari penjual bahwa barang telah dikirimkan atau pembayaran belum dilakukan. Dibutuhkan informasi untuk memastikan siapa pengirim dan penerimanya
4. privasi, pelanggan menginginkan agar identitas mereka aman. Mereka tidak ingin orang lain mengetahui apa yang mereka beli
5. keselamatan, pelanggan menginginkan jaminan bahwa aman untuk memberikan informasi nomer kartu kredit di internet.

Terdapat beberapa ancaman yang terjadi dalam sistem *e-commerce* adalah [13]:

1. System Penetration, yaitu seseorang yang tidak berhak dapat mengakses sistem komputer dan dapat melakukan segalanya.
2. Authorization Violation, yaitu penyalahgunaan wewenang yang dimiliki oleh seseorang yang berhak.
3. Planting, yaitu melakukan penyerangan secara terencana, misalnya memasukkan Trojan Horse dan melakukan penyerangan dengan waktu yang telah ditentukan sebelumnya.
4. Communications Monitoring, yaitu melakukan monitoring semua informasi rahasia.
5. Communications Tampering, yaitu mengubah pesan di tengah jalan oleh penyerang di dalam proses transimisi data dan mengganti sistem server dengan sistem server yang palsu.

6. Denial of Service (DoS), yaitu menolak layanan terhadap client yang berhak.
7. Repudiation, yaitu menolak aktivitas transaksi karena suatu hal yang disengaja atau kesalahan teknis.

Beberapa metode dan mekanisme yang dapat digunakan untuk memenuhi dimensi keamanan *e-commerce* diatas, yaitu [14]:

1. Public Key Infrastructure (PKI). Memungkinkan para pemakai yang pada dasarnya tidak aman di dalam jaringan publik seperti Internet, maka dengan PKI akan merasa aman dan secara pribadi menukar uang dan data melalui penggunaan suatu publik.
2. Public Key Algorithm. Disebut juga dengan algoritma asimetris (Asymmetric Algorithm) yaitu algorima yang menggunakan kunci yang berbeda pada saat melakukan enkripsi dan melakukan deskripsi.
3. Digital Signature. Tanda tangan digital merupakan tanda tangan yang dibuat secara elektronik, dengan jaminan yang lebih terhadap keamanan data dan keaslian data, baik jaminan tentang indentitas pengirim dan kebenaran dari data atau paket data terebut.
4. Certificate Digital. Sertifikat Otoritas merupakan pihak ke-tiga yang bisa dipercaya (Trust Thrid Party/TTP). Sertifikat Otoritas yang akan menghubungkan kunci dengan pemiliknya. TTP ini akan menerbitkan sertifikat yang berisi identitas seseorang dan juga kunci privat dari orang tersebut.
5. Secure Socket Layer (SSL). Suatu protokol yang membuat sebuah pipa pelindung antara browser cardholder dengan merchant, sehingga pembajak atau penyerang tidak dapat menyadap atau membajak informasi yang mengalir pada pipa tersebut. Pada penggunaannya SSL digunakan bersaman dengan protokol lain, seperti HTTP (Hyper Text Transfer Protocol), dan Sertificate Autority.
6. Transport Layer Security (TLS). Adalah protokol cryptographic yang menyediakan keamanan komunikasi pada Internet seperti e-mail, internet faxing, dan perpindahan data lain.
7. Secure Electronic Transaction (SET). Merupakan gabungan antara teknologi public/private key dengan digital signature. Pada enkripsi, public key menggunakan enkripsi 56 bit sampai dengan 1024 bit, sehingga tingkat kombinasi enkripsinya pun sangat tinggi. Didalam bertransaksi, CA membuatkan sertifikat digital yang berisi informasi jati diri dan kunci publik cardholder, berikut informasi nomor kartu kredit yang ‘disembunyikan’,sehingga cardholder seperti mempunyai “KTP” digital. Biaya pengembangan infrastruktur SET relative sangat mahal, sehingga ini merupakan salah satu kerugiannya.

Regulasi Keamanan Data Pribadi

Konsep provasi yang merupakan dasar dari data pribadi, sebagai suatu hak asasi manusia yang harus dilindungi diakui dalam Pasal 12 Deklarasi Umum Hak Asasi Manusia (1948), yang menyatakan bahwa:

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attack” (Tidak ada seorang pun dapat diganggu dengan sewenang-wenang urusan pribadi, keluarga, rumah tangga atau hubungan surat menyuratnya, juga tidak diperkenakan pelanggaran atas kehormatan dan nama baiknya. Setiap orang berhak mendapat perlindungan hukum terhadap gangguan atau pelanggaran itu)”.

Ketentuan tersebut selanjutnya dipertegas dalam Pasal 17 Konvenan Internasional Tentang Hak -hak Sipil dan Politik (1966), yang menyatakan bahwa:

“(1) No one shall be subjectedto arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation; (2) Everyone has the right to protection of the law against such interference or attack”

(1) Tidak boleh seorangpun yang dapat secara sewenang-wenang atau secara tidak sah dicampuri masalah-masalah pribadinya, keluarganya, rumah atau hubungan surat menyuratnya, atau secara tidak sah diserang kehormatan dan nama baiknya;(2) Setiap orang berhak atas perlindungan hukum terhadap campur tangan atau serangan.

Untuk memastikan tingkat perlindungan yang konsisten bagi perorangan di seluruh dunia dan untuk mencegahnya divergensi yang menghambat pergerakan bebas data pribadi di dalam pasar internal. Diperlukan regulasi memberikan kepastian hukum dan transparansi bagi pelaku ekonomi, termasuk mikro, kecil, dan menengah perusahaan, dan untuk memberikan orang perseorangan di semua Negaradengan tingkat yang sama dari hak yang dapat diberlakukan secara hukum dan kewajiban dan tanggung jawab untuk pengontrol dan prosesor, untuk memastikan pemantauan yang konsisten dari pemrosesan data pribadi, dan sanksi yang setara.

Regulasi kemanan data pribadi berakar pada fondasi ganda: di satu sisi, bertujuan untuk memfasilitasi aliran

bebas data pribadi; di sisi lain, ini berfungsi untuk lebih melindungi hak-hak dasar individu, dengan fokus pada hak atas privasi dan perlindungan data [14]. Secara khusus, regulasi kemanan data pribadi memberikan perlindungan khusus terhadap beberapa jenis data pribadi yang dianggap sensitif berupa informasi terkait etnis, pilihan politik, agama atau kepercayaan atau keanggotaan pada organisasi perdagangan, data biometrik untuk tujuan mengidentifikasi seseorang, data kesehatan atau kehidupan sex atau orientasi sexual. Terhadap data sensitif tersebut dilarang untuk diproses kecuali memenuhi serangkaian persyaratan yang dicantumkan secara eksplisit dalam regulasi, antara lain persetujuan tertulis dari pemilik data dan pengumpulan data dibatasi hanya pada tujuan-tujuan yang telah tercantum secara definitif dalam regulasi tersebut [15].

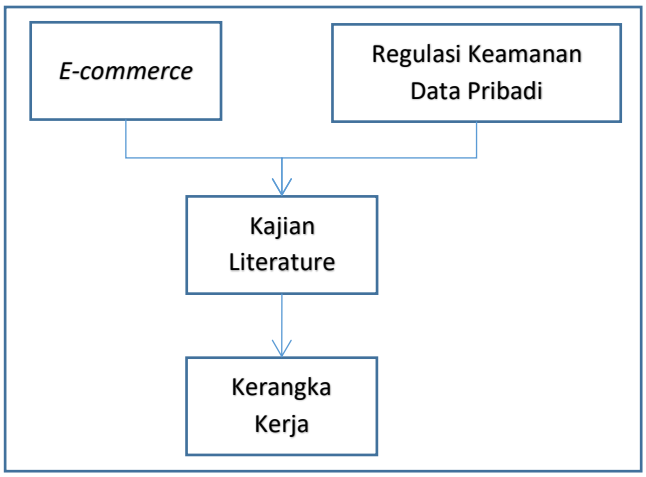
Alasan perlindungan data pribadi sangat jelas dari kerangka peraturan. Data pribadi hanya mengacu pada orang yang mencirikan mereka seperti itu. Oleh karena itu, apabila pembeli membeli mobil, maka mobil tersebut adalah miliknya yang dapat dibuktikan dengan tanda terima dan / atau perjanjian yang ditandatangani. Data pribadi adalah milik perorangan, dan karenanya tidak dapat dicabut. Namun, dengan perkembangan teknologi dan Internet, data pribadi menjadi semakin terbuka dan dapat diakses oleh mereka yang dapat menggunakannya untuk tujuan mereka sendiri yang melanggar hukum. Jejaring sosial dapat menjadi contoh umum. Menurut informasi statistik media sosial dari Februari 2017, jumlah pengguna jejaring sosial dengan data pribadi mencapai 4,6 miliar. Jumlah ini juga termasuk apa yang disebut profil pengguna palsu yang mewakili duplikat profil asli (orang) yang dimaksudkan untuk merugikan mereka dengan menggunakan data pribadi mereka (nama depan, nama belakang, foto, video, dll.)

Regulasi kemanan data pribadi di era ekonomi digital setidaknya harus memenuhi 3 kriteria [16]:

1. Memiliki karakter internasional. Dalam suatu transaksi ekonomi antar individu dan perusahaan, tempat penyimpanan fisik privasi dan data pribadi akan sulit ditemukan apabila transaksi dilakukan secara digital. Tempat penyimpanan data tersudut tidak dapat dibatasi lagi oleh lingkup yurisdiksi nasional, karena akan dapat bersifat lintas negara. Beberapa instrumen hukum internasional mengatur prinsip-prinsip privasi dan data pribadi yang diakui secara internasional. Prinsip-prinsip tersebut merupakan fondasi bagi hukum perlindungan data nasional yang modern.
2. Melindungi privasi dan data pribadi sebagai hak positif.
3. Merupakan elemen perekat individu dan masyarakat ekonomi. Dalam masyarakat era ekonomi digital privasi juga merupakan sebuah hak yang dapat melekatkan individual dengan masyarakat. Dengan adanya perlindungan privasi dan data pribadi maka individu akan memiliki kepercayaan untuk berpartisipasi menjadi masyarakat era ekonomi digital.

III. METODE

Metode penulisan yang digunakan dalam pembuatan paper ini adalah dengan mencari bahan dan informasi yang berhubungan dengan topik dari sumber-sumber literatur, baik dari buku, jurnal, maupun artikel-artikel dari situs serta observasi seperti pada Gambar 1.



Gambar 1. Metode Penulisan

Tahap awal yang dilakukan adalah kajian tentang e-commerce baik itu definisi, menfaat dan hal yang berkaitan dengan kemanan data pribadi yang ada. Selanjutnya dilakukan kajian serta observasi terhadap regulasi yang berkaitan dengan keamanan data pribadi di Indonsia. Tahap selanjutnya dari penulisan ini adalah memberikan kerangka kerja tentang regulasi keamanan data pribadi pada e-commerce.

IV. HASIL DAN PEMBAHASAN

Indonesia telah memiliki regulasi kemanan data pribadi yang terdapat di beberapa peraturan perundang-undangan, diantaranya

a. Undang-Undang No. 36 Tahun 2009 tentang Kesehatan mengatur tentang rahasia kondisi pribadi pasien

b. Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan mengatur privasi dan data pribadi mengenai nasabah penyimpan dan simpanannya.
c. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi.
d. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.
e. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan telah diubah dengan Undang-Undang No. 24 Tahun 2013)
f. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (telah diubah dengan Undang-Undang Nomor 19 Tahun 2016), melarang penggunaan informasi diperoleh melalui media elektronik yang memuat privasi pada data pribadi yang terkait dengan sebuah individu tanpa persetujuan tersebut orang. UU ITE selanjutnya mengatur hal itu siapapun dengan sengaja dan tanpa harus sah hak dilarang berubah, menambahkan, mengurangi, mentransmisikan, menghancurkan, menghilangkan, mentransfer atau menyembunyikan elektronik informasi dan / atau dokumen elektronik dimiliki oleh orang lain atau dimiliki oleh publik.

Indonesia pada dasarnya juga telah memiliki Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi yang kini masih dalam tahap pembahasan intra Kementerian dan diharapkan dapat segera diusulkan dalam prolegnas 2018. Namun hingga kini belum terealisasi. Konvergensi Perlindungan Data Pribadi penting bagi Indonesia belum terlaksana, padahal konvergensi tersebut penting untuk memberikan perlindungan privasi dan data pribadi yang setara dengan negara-negara lain. Pengaturan yang akan disusun dalam Rancangan Undang-Undang diharapkan akan menempatkan Indonesia sejajar dengan negara-negara dengan tingkat perekonomian yang setara atau lebih maju, yang telah mengimplemntasikan regulasi mengenai keamanan data pribadi. Kekosongan regulasi ini tentu saja membawa implikasi terhadap kemanan data pribadi.

Regulasi kemanan data pribadi harus dipertimbangkan sebagai salah satu bidang yang paling penting yang dibutuhkan oleh Indonesia. Ini merupakan isu yang penting dalam komunitas modern karena perlindungan data pribadi akan mempengaruhi cara berkomunikasi dan cara-cara baru dalam bertransaksi khususnya dalam *e-commerce*. Indonesia harus segera membentuk suatu sistem hukum yang dapat menjamin kepastian hukum namun tetap memperhatikan kesiapan masyarakat dalam menghadapi nilai-nilai baru [16]. Nilai baru yang dimaksud di sini adalah kemajuan teknologi yang menghendaki adanya kemanan data pribadi pengguna khususnya dalam menghadapi perkembangan *e-commerce*.

Jadi penyusunan undang-undang dapat mengakomodasi beberapa kepentingan: pertama, melindungi privasi masyarakat atas informasi pribadi, kedua, memperlancar hubungan perdagangan internasional khususnya *e-commerce* dengan mengikuti standar pengaturan internasional dengan menyesuaikan dengan keadaan masyarakat Indonesia.

Selain pendekatan regulasi, Lawrence Lessig berpendapat bahwa ada pendekatan lain selain pendekatan hukum yang dapat digunakan sebagai salah satu mekanisme perlindungan terhadap transaksi di *e-commerce* yaitu melalui mekanisme pasar (market-based solution) [18]. Mekanisme pasar menawarkan solusi atas problem yang dihadapi untuk mengatur kegiatan ekonomi. Mekanisme ini tidak membutuhkan kekuasaan yang besar untuk menentukan apa yang harus dikonsumsi dan diproduksi. Sebaliknya, tiap individu dibebaskan untuk memilih sendiri apa yang ia butuhkan dan bagaimana memenuhinya.

Praktik ini diterapkan dalam pengaturan privasi pada lalu lintas *e-commerce* di Amerika Serikat dan Singapura. Kedudukan konsumen (dalam hal ini adalah pengguna *e-commerce*) dalam pendekatan mekanisme pasar dalam lalu lintas *e-commerce* adalah bahwa konsumen tidak lagi memiliki kemampuan dan kewenangan untuk mengawasi penyebaran informasi pribadinya. Karena oleh itu, pihak penyedia jasa *e-commerce* dapat mengakses, memproses, dan menyebarluaskan tanpa persetujuan pemilik informasi. Pengaturan ini dikoordinasikan oleh asosiasi industri.

Untuk menerapkan prinsip keseimbangan para pihak dalam pengaturan ini, maka pihak industri biasanya menaikkan daya tawar mereka dengan menyatakan bahwa jasa layanan yang mereka kelola terjaga keamanannya. Pengaturan ini juga diterapkan oleh negara Amerika Seikat dan Singapura. Akan tetapi, ternyata di dalam praktiknya, hal ini sulit untuk diterapkan secara efektif karena tidak ada lembaga yang secara khusus dapat mengawasi tindakan pihak penyedia jasa *e-commerce*.

Pendekatan mekanisme pasar ini sebenarnya sangat baik jika dapat diterapkan di Indonesia. Pendekatan ini dapat mendorong pihak penyedia jasa *e-commerce* turut bertanggung jawab melindungi privasi penggunanya Asalkan di dalam pelaksanaannya, ada lembaga pengawas yang menerapkan prinsip-prinsip pemanfaatan informasi secara adil dan mempunyai wewenang untuk menjatuhkan sanksi.

Konsep regulasi yang baik seharusnya meliputi: prinsip, aturan, proses, dan institusi. Jika dikaitkan dengan konsep regulasi kemanan data pribadi maka harus [16]:

1. Prinsip yang menjadi dasar dalam menetapkan peraturan harus mempertimbangkan baik nasional maupun internasional perkembangan. Prinsip dari privasi informasi pada data pribadi regulasi harus didasarkan pada UUD 1945 dimana Pasal 28 (G) memiliki jelas mengakui bahwa hak untuk keamanan pada data pribadi harus dilindungi.
2. Prinsip informasi yang adil yang membutuhkan standar praktik diperlukan untuk memastikan bahwa entitas yang mengumpulkan dan menggunakan data pribadi yang memadai dalam hal pengamanan data pribadi.
3. Harus jelas definisi dari istilah substansial menjadi disebutkan dalam regulasi.
4. Dewan Pengawas dalam mencapai konsep regulasi yang baik, keterlibatan kedua institusi dan proses adalah suatu keharusan.

V. KESIMPULAN

Penerapan keamanan data pribadi di *e-commerce* pada saat ini merupakan salah satu syarat yang layak dipenuhi. Dengan *E-commerce* memungkinkan bertransaksi dengan cepat dan biaya yang murah tanpa melalui proses yang berbelit-belit. Walau dalam penerapannya masih banyak terdapat ancaman pada keamanannya, tetapi untuk kedepannya diharapkan bisnis *E-commerce* dapat terus berkembang tentunya sejalan dengan perkembangan keamanannya.

Indonesia telah memiliki regulasi kemanan data pribadi yang terdapat di beberapa peraturan perundang-undangannya Namun hingga saat ini, hanya terdapat Rancangan Peraturan Pemerintah tentang *E-commerce* (RPP *E-commerce*) tentang Perubahan atas Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Selama rancangan peraturan tersebut belum disahkan, maka kerangka utama peraturan perundang-undangan terkait kegiatan *e-commerce* masih mengacu pada Undang-Undang No. 11 tahun 2008 tentang Informasi dan Elektronik (UU ITE).

Regulasi kemanan data pribadi harus dipertimbangkan sebagai salah satu bidang yang paling penting yang dibutuhkan oleh Indonesia. Ini merupakan isu yang penting dalam komunitas modern karena perlindungan data pribadi akan mempengaruhi cara berkomunikasi dan cara-cara baru dalam bertransaksi khususnya dalam *e-commerce*. Konsep regulasi yang baik seharusnya meliputi: prinsip, aturan, proses, dan institusi. Yaitu berupa prinsip yang mempertimbangkan baik perkembangan nasional maupun internasional, prinsip dari privasi informasi pada data pribadi, prinsip informasi yang adil, jelas definisi dari istilah substansial menjadi disebutkan dalam regulasi dan terdapatnya dewan pengawas.

DAFTAR PUSTAKA

[1] APJI "Pengguna & Prilaku Internet Indonesia". Hal 1-7 .Edisi 23 April 2018.

[2] M.M. Belalawe. "Tinjauan Keamanan Sistem Transaksi Dan Pembayaran Pada E-Commerce Studi Kasus Toko Online www.buahonline.com". Program Studi Teknik Informatika, STIKOM Artha Buana Kupang. Seminar Nasional Teknologi Informasi dan Komunikasi, 2013.

[3] Emmy Febriani Thalib, dkk. "Tijnjauan Yuridis Menegnai Marketplace Berdasarkan Peraturan Perundang-Undnagan di Indonesia". Volume 7 No. 2. STMIK STIKOM Indonesia, 2019

[4] Shahriari, et al. "*E-commerce* and it impacts on global trend and market. International journal of research-Granthaalayah". (3)4, pp 49-55, 2015.

[5] Khan, A., G. "Electronic Commerce, A Study on Benefits and Challenges in an Emerging Economy". Global Journal of Management and Business Research: B Economics and Commerce, (16)1, 2016

[6] Mariah, dkk. "Analisis Faktor-Faktor Yang Mempengaruhi Jaminan Keamanan Dalam Transaksi Dengan Menggunkan Sistem E Commerce Pada Bajiki Store Makassar". STIE Nobel Indonesia Makassar, 2017.

[7] Radi Petrov Romansky. "Social Media and Personal Data Protection". Technical University of Sofia, pp 72. 2014.

[8] Juyoen Lee et al. "Personal data protection of academic journals in the age of the European General Data Protection Regulation, guidelines for Korean journals". College of Law, Dongguk University, Seoul, Korea, pp 73-77, 2019

[9] https://ec.europa.eu/info/law/law-topic/data protection/reform/what-personal-data_en., 14 Januari 2021.

[10] I Gusti Ngurah Indra Saputra, dkk. "Pengembangan Sistem Keamanan untuk *E-commerce"*. MERPATI VOL. 5, NO. 1 Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Udayana Bali, 2017.

[11] R. A., Esti, Kurniati, A. "Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada E-Voting di Indonesia". UPN Veteran Yogyakarta, 2009.

[12] Andre M. R. Wajong, Carolina Rizki Putri. "Kemanan Dalam Elektronik Commerce". ComTech Vol.1 No.2. Jurusan Teknik Industri, Fakultas Sains dan Teknologi, Bina Nusantara University. pp 867-874, 2010.

[13] W. Purbo, Onno, dkk. "Mengenal E-Commerce". Elex Media Komputindo Jakarta, 2001.

[14] Lynskey, O. "The dual objectives of European data protection regulation. In The Foundations of EU Data Protection Law". Oxford, UK, Oxford University Press, 2015.

[15] Siti Yuniarti. "Perlindungan Hukum Data Pribadi". JURNAL BECOSS (Business Economic, Communication, and Social Sciences), Vol.1, No.1, Business Law Program, Law Department,

Faculty of Humanities, Bina Nusantara University, pp 147-154, September 2019.
[16] Sinta Dewi Rosadi. “Protecting Privacy On Personal Data In Digital Economic Era, Legal Framework In Indonesia”. Faculty of Law, University of Padjadjaran, Bandung. Indonesia. pp 150-155, 2017
[17] Lili Rasjidi dan I. B. Wyasa Putra. “Hukum Sebagai Suatu Sistem, Remaja Rosdakarya”, Bandung, 2003.
[18] Sinta Dewi. “Privasi atas Data Pribadi, Perlindungan Hukum dan Bentuk Pengaturan di Indonesia”. Jurnal De Jure, Vol. 15 Nomor 2, Juni 2015.